



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002044071 A**(43) Date of publication of application: **08.02.02**

(51) Int. Cl.

H04L 9/16
H04L 9/08
H04N 5/44
H04N 5/765
H04N 5/91
H04N 7/16
H04N 7/167

(21) Application number: **2000370282**(22) Date of filing: **05.12.00**(30) Priority: **16.05.00 JP 2000148600**(71) Applicant: **HITACHI LTD**

(72) Inventor: **HARADA HIROMI**
KONISHI KAORU
YAMAZAKI IORI

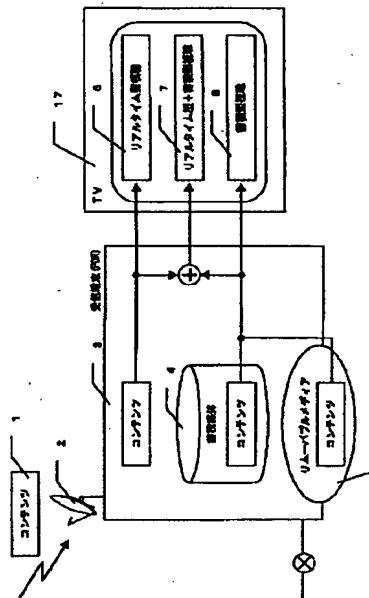
(54) RECEIVING METHOD

COPYRIGHT: (C)2002,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To protect a copyright by enciphering various contents with another key and making portable a restricted receiving (CA) module.

SOLUTION: For performing enciphering for each of contents, the contents are enciphered on the transmitting side, meta-data are transmitted simultaneously with the enciphered contents, and the enciphered contents and the meta-data are stored on the side of a receiving terminal, which receives contents information. When viewing the stored enciphered contents, the meta-data are enciphered while using a disposable key prepared inside the receiving terminal and the enciphered contents and the meta-data are separated. In the case of transfer to a third person, the personal information of the transfer destination first received without including owner information is stored. Since enciphering is enabled for each of contents by a unique key and a second CA module capable of specifying an individual is combined, service providing to an individual and transfer to the third person are enabled.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-44071

(P2002-44071A)

(43)公開日 平成14年2月8日(2002.2.8)

(51)Int.Cl. ⁷	識別記号	F I	キーワード(参考)
H 0 4 L 9/16		H 0 4 N 5/44	Z 5 C 0 2 5
9/08		7/16	C 5 C 0 5 3
H 0 4 N 5/44		H 0 4 L 9/00	6 4 3 5 C 0 6 4
5/765			6 0 1 A 5 J 1 0 4
5/91			6 0 1 E

審査請求 未請求 請求項の数10 O L (全 30 頁) 最終頁に続く

(21)出願番号 特願2000-370282(P2000-370282)

(22)出願日 平成12年12月5日(2000.12.5)

(31)優先権主張番号 特願2000-148600(P2000-148600)

(32)優先日 平成12年5月16日(2000.5.16)

(33)優先権主張国 日本 (J P)

(71)出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72)発明者 原田 宏美
東京都千代田区神田駿河台四丁目6番地
株式会社日立製作所放送・通信システム推進事業部内

(72)発明者 小西 薫
東京都千代田区神田駿河台四丁目6番地
株式会社日立製作所放送・通信システム推進事業部内

(74)代理人 100107010
弁理士 橋爪 健

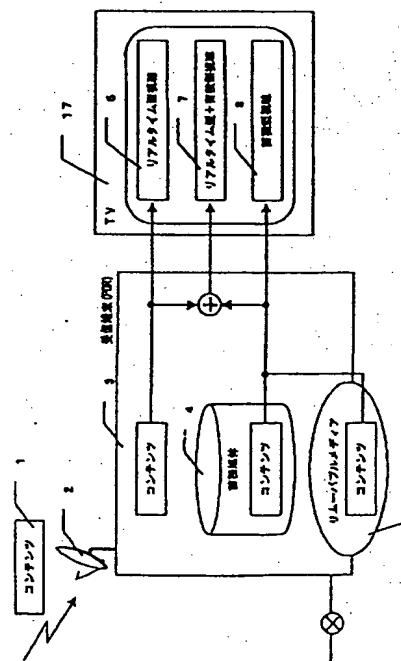
最終頁に続く

(54)【発明の名称】 受信方法

(57)【要約】

【課題】 様々なコンテンツに別の鍵で暗号をかけ、限定受信 (C A) モジュールを可搬可能とし、著作権を保護する。

【解決手段】 コンテンツ毎の暗号化を行うために、送信側でコンテンツを暗号化し、暗号化されたコンテンツと同時にメタデータを送信し、コンテンツ情報を受信した受信端末側で暗号化コンテンツとメタデータ蓄積を行う。蓄積された暗号化コンテンツを視聴する際に、メタデータに、受信端末内で作成した使い捨て鍵を用いて暗号化し、暗号化コンテンツとメタデータの分離化を行う。また、第3者への譲渡に対しては、所有者情報を入れずに最初に受け取った譲渡先の個人情報に格納される。コンテンツ毎にユニークな鍵で暗号化可能とし、個人を特定できる第2の C A モジュールを組み合わせることで、個人に対するサービス提供、第3者への譲渡を可能とする。



【特許請求の範囲】

【請求項1】 選択されたコンテンツに対応する暗号化メタデータを第1の使い捨て鍵(K1)で復号するステップと、

メタデータに基づきコンテンツの視聴可否を判断し、課金情報を含む契約情報を作成し、メタデータに含めるステップと、

作成されたメタデータを第1及び第2の分離メタデータに分離するステップと、

第2の使い捨て鍵(K1')を生成するステップと、

第2の分離メタデータを第2の使い捨て鍵(K1')で暗号化した第2の分離メタデータを生成し、記録媒体及びリムーバブルメディアに蓄積するステップと、

第1の分離メタデータに第2の使い捨て鍵(K1')を含め、入力された第3の個人鍵(Km2)で暗号化し、第2のモジュールに記録するステップと、

記録媒体に蓄積された暗号化コンテンツをリムーバブルメディアに蓄積するステップとを含む受信方法。

【請求項2】 メタデータは、検索情報及び/又は課金情報を含む契約情報を含み、契約情報に従い、コンテンツ毎に課金処理を行うことを特徴とする請求項1に記載の受信方法。

【請求項3】 第1のモジュールは受信機内に備えられ、第2のモジュールは可搬形で受信機に脱着可能であることを特徴とする請求項1又は2に記載の受信方法。

【請求項4】 第1の受信機により暗号化された第1の分離メタデータ及び第3の個人鍵(Km2)が記録された第2のモジュール、及び、コンテンツ鍵(Kk)を含む暗号化された第2の分離メタデータ及び暗号化コンテンツが蓄積されたリムーバブルメディアを第2の受信機に装着するステップと、

第2のモジュールに記録された暗号化された第1の分離メタデータを第3の個人鍵(Km2)で復号化して第1の分離メタデータを生成し、

第1の分離メタデータに含まれた第2の使い捨て鍵(K1')を用いて復号化して第2の分離メタデータを生成するステップと、

第1及び第2の分離メタデータに基づいてコンテンツの視聴の可否を判断するステップと、

復号化された第2の分離メタデータに含まれるコンテンツ鍵(Kk)を用いてリムーバブルメディアに記録された暗号化コンテンツを復号化してコンテンツを生成するステップを含む請求項1乃至3のいずれかに記載の受信方法。

【請求項5】 選択されたコンテンツに対応する暗号化メタデータを第1の使い捨て鍵(K1)で復号するステップと、

メタデータに基づきコンテンツの視聴可否を判断し、課金情報を含む契約情報を作成し、メタデータに含めるステップと、

作成されたメタデータを第1及び第2の分離メタデータに分離するステップと、

ギフト鍵を生成し、リムーバブルメディアに蓄積するステップと、

第2の分離メタデータをギフト鍵で暗号化し、リムーバブルメディアに蓄積するステップと、

第1の分離メタデータに第2の使い捨て鍵(K1')を含め、入力された第2の個人鍵(Km2)で暗号化し、第2モジュールに記録するステップと、

記録媒体に蓄積された暗号化コンテンツをリムーバブルメディアに蓄積するステップとを含む請求項1乃至3のいずれかに記載の受信方法。

【請求項6】 リムーバブルメディアに記録された暗号化された第2の分離データを復号化し、第2の分離メタデータを生成するステップと、

第2のモジュールに記録された暗号化された第1の分離メタデータを復号化し、第1の分離メタデータを生成するステップと、

第1及び第2の分離メタデータに基づき、コンテンツの視聴可否を判断するステップと、

リムーバブルメディアに記録された暗号化コンテンツを、コンテンツ鍵で復号化してコンテンツを生成するステップとを含む請求項1乃至5のいずれかに記載の受信方法。

【請求項7】 コンテンツを、メタデータと同一の鍵で暗号化して、その鍵をコンテンツ配信時とは別の時間帯、別の配信場所又は別の配信手段で配信することを特徴とする請求項1乃至6のいずれかに記載の受信方法。

【請求項8】 暗号化コンテンツをリムーバブルメディアに蓄積する際、記録媒体内の暗号化コンテンツ及び暗号化メタデータを複写して使用することを特徴とする請求項1乃至7のいずれかに記載の受信方法。

【請求項9】 受信機内の第1のモジュールに記憶された第2の個人鍵(Km1)を用いて、受信されたスクランブル鍵(Ks)を復号化し、スクランブル鍵(Ks)を用いて復号化することにより、暗号化コンテンツ及び暗号化メタデータを含むイベントを生成するステップと、

受信機内に記憶された第1の個人鍵(Kmc)を用いて、受信された第1の暗号化ワーク鍵(Kwc')を復号化して第1のワーク鍵(Kwc)を生成するステップと、

復号化された第1のワーク鍵(Kwc)を用いて、共通情報として受信された第1の暗号化コンテンツ鍵(Kk')を復号化して第1のコンテンツ鍵(Kk)を生成するステップと、

暗号化メタデータを第1のワーク鍵(Kwc)で復号化してメタデータを生成するステップとをさらに含む請求項1乃至8のいずれかに記載の受信方法。

【請求項10】 受信機内の第1のモジュールに記憶された第2の個人鍵(Km1)を用いて、受信されたスクランブル鍵(Ks)を復号化し、スクランブル鍵(Ks)を用いて暗号

化コンテンツ及び暗号化メタデータを含むイベントを生成するステップと、

受信機内に記憶された第1の個人鍵(Kmc)を用いて、受信された第1の暗号化ワーク鍵(Kwc')を復号化し第1のワーク鍵(Kwc)を生成するステップと、

復号化された第1のワーク鍵(Kwc)を用いて、暗号化メタデータを復号化し、そこに含まれた第1のコンテンツ鍵(Kk)を求めるステップとをさらに含む請求項1乃至8のいずれかに記載の受信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、受信方法に係り、特に、デジタル放送により暗号化コンテンツを視聴するための受信方法に関する。

【0002】

【従来の技術】従来のデジタル放送では、サービスチャンネル毎に視聴可／不可の契約を行う契約形態、もしくは同一チャンネル内での時間毎の番組契約を行う契約形態が存在していた。また、既存のデジタル放送等では、各々のコンテンツ単位でのコンテンツの購入を行わせるために、ユーザーがサービス選択後に欲しいコンテンツを選択、契約又は決定し、その契約又は決定と同時にセンタ側との通信を行うようにしている。ユーザーとセンタ側とのリアルタイム通信によって各コンテンツの購入を確認し、確認後契約者に購入許可データを送信することで、ユーザーはコンテンツを購入可能となる。このような双方向リアルタイム購入方式でコンテンツ単位での販売が行われることとなる。

【0003】暗号化に関しては、今後始まるデジタル放送において、ネットワーク内で使用可能な暗号鍵は数が固定されているため、伝送路で暗号化する／しないの判断がなされる。また、現在の伝送方式では、センタ側で暗号化されたコンテンツは、受信端末内で受信後直に暗号解除を行った後に蓄積装置等に記録される。このように伝送時におけるコンテンツの暗号化は、現在1次暗号のみで行なわれている。

【0004】

【発明が解決しようとする課題】しかしながら、従来のデジタル放送では、契約時間内での全てのサービス情報を取得することができるが、ユーザーが選択したサービス情報のみの視聴もしくはコンテンツのみの入手は困難である。

【0005】また、従来のCS／BSなどのデジタル放送でのサービスにおいては、契約形態がチャンネル視聴可／不可、または同一チャンネル内の番組視聴可／不可の契約提供がメインとなっている。これはデジタル放送内における暗号化に用いる鍵の数の制限があるためである。ただし複数の鍵を使用すると鍵の管理が複雑となるだけでなく、複数鍵でのコンテンツの暗号化を行うことで暗号を解くために必要な情報の常時送信となり、現在

の伝送量よりさらに多くの情報を伝送しなくてはならない。これは少ない伝送領域においては、困難に近く現実的ではない。また、日々増加するコンテンツ毎に鍵をかけることは、鍵の数が無限大に近くなることであり、これも管理が非常に難しい。さらに、リアルタイム復号に必要な情報を常に伝送しているため、受信端末は、受信時に復号化に必要なICカード等のモジュール(CA(Conditional Access, 限定受信)モジュール)を常時取り付けさせる必要がある。これらのことより、同じチャンネル内の同じ番組の同じ時間において複数の鍵を用いてコンテンツの暗号化を行うことは、困難に近い。

【0006】また、従来の受信端末では、暗号解除後に再度受信端末内で暗号化を行うことが出来ない。これより受信端末等に存在する蓄積コンテンツを一度復号化した後に、再度暗号化させて蓄積をさせることは不可能であり、また伝送路の暗号化のまま蓄積すると蓄積時における暗号化の鍵扱い等がむずかしくなり、暗号化させて蓄積させるには信頼性等様々な課題が多い。また、デジタル放送を受信する場合において視聴可／不可等の契約を扱う情報が受信端末毎でしか行えないため、受信端末を利用するユーザーが複数の場合、センタ側で複数ユーザー毎の契約形態を認識できない等の課題がある。

【0007】さらに、例えばコンテンツの第3者に対する譲渡場合等において要求される、著作権保護の方式として電子透かし等のパスワード埋め込みの形式は存在するが、全てのデータ形式に対して有効ではなく、コンテンツのみの保護でしかない。システムとしてコンテンツ並びにコンテンツ関連情報(メタデータ)の両方を保護する方式は現状存在しない。

【0008】本発明は以上のような課題を解決することを目的とする。例えば、本発明は、受信端末内で生成した使い捨て鍵を用いてメタデータの作成並びに分割化を行うことで、コンテンツ毎に暗号化可能とする。また、本発明によると、個人を特定できる第2のCAモジュールを合わせることで個人特定のサービスを行うようにすることを目的とする。

【0009】さらに、本発明は、メタデータ内にコンテンツの所有者情報を入れずにおくことで、コンテンツの譲渡をされた方の受け取り時に初めてコンテンツ所有者が特定できるようにし、CAモジュールへの所有者情報記入が行なわれることにより、第3者への譲渡目的としたコンテンツサービスを実現することを目的とする。

【0010】

【課題を解決するための手段】本発明は、暗号化コンテンツとそのコンテンツの視聴のために必要なコンテンツ関連情報であるメタデータとによりコンテンツを定義し、また、個人を特定した第2のCAモジュールを使用する。これにより、個々に対するサービスの提供を可能とし、また第3者に対する譲渡を目的としたコンテンツの受け渡しにおけるセキュリティ保護も施し、第3者に

譲渡を行うサービスの提供を可能とする。

【0011】ここで、メタデータとは、基本的にコンテンツ以外の情報の総称であり、例えば、コンテンツ制御情報、コンテンツ内容情報、コンテンツ関連情報として定義することができる。概念的には受信端末側でコンテンツを制御するための情報で、例えばコンテンツの蓄積予約を行うための情報（EPG（Electronic Program Guide、電子番組ガイド）に表示するためのコンテンツの名前、ジャンル、配信場所、配信予定日時）、利用制限情報（視聴が可能となるための条件、20歳以上、男性、〇〇放送局との契約者）、暗号の鍵等の情報が含まれる。

【0012】本発明においては、コンテンツ毎の暗号化を行なうために、暗号化コンテンツとそのコンテンツに対する視聴契約形態等の情報を含むコンテンツ関連情報（メタデータ）の分離化を行なう。最初に送信側でコンテンツの暗号化を行ない、暗号化されたコンテンツと同時にメタデータを送信する。この情報を受信した受信側の受信端末では暗号化コンテンツの蓄積、メタデータの伝送路における伝送暗号の復号化および受信端末内で生成される使い捨て鍵による暗号化等の加工を必要に応じて行なった後、送信データの全ての蓄積を行なう。蓄積された暗号化コンテンツを視聴する際は、使い捨て鍵により暗号化されたメタデータを復号化し、有効期限、視聴回数制限、コピー制限、暗号化されたコンテンツを復号するための情報などを埋め込み、再び受信端末内で生成した使い捨て鍵を用いて、メタデータを元にメタデータ1、2の作成並びに分割化を行なう。暗号化コンテンツとメタデータ2をセットとして受信端末の記録媒体等に蓄積し、また残りのメタデータ1をCAモジュール等のユーザー個人特定蓄積媒体に書込む。

【0013】このように、メタデータ1、2と暗号化コンテンツを合わせることで初めて視聴可能となるシステムとする。また、暗号化コンテンツと共に蓄積されるメタデータは受信端末内で生成される使い捨て鍵で受信端末内で暗号化を行なう。CAモジュールに書込むメタデータ1はユーザー個人の鍵でCAモジュール内で暗号化を行なってもいいし、受信端末内でのコンテンツ管理機能で暗号化を行うことも可能である。また、暗号化を行わずにCAモジュール内に格納も可能である。受信端末側では、使い捨て鍵を生成しコンテンツ関連情報（メタデータ）に再度暗号化を行なうことで、コンテンツ毎に異なった暗号化を行なうことを可能とする。

【0014】ユーザーが契約コンテンツを視聴する際には、検索／課金情報等、受信端末側でこれらの情報を生成し、受信端末内でメタデータ1、2などに基づき再生を行なう。よって受信端末内で複数の鍵を生成し、コンテンツ毎に暗号用の鍵として使用が可能となる。また、暗号化されたコンテンツをセンタ側より送信することで、受信端末内で大容量のコンテンツを暗号化する必要

はなく、メタデータ、受信端末内で生成されるメタデータ1、2についてのみ使い捨て鍵や個人鍵で暗号化する。このメタデータの情報の解読で復号に必要な情報入手可能となる。さらにコンテンツ毎に鍵が異なるが、この異なった鍵の全てがCAモジュール等へ書込まれる。この書込まれた鍵の情報を使用して暗号化コンテンツの再生等を行なうが、再生時のみCAモジュール等を必要とするため、常時受信端末に設置する必要はなく、家庭でのコンテンツ購入だけでなく外部などの家庭外への持ち出しでのコンテンツの視聴契約が可能となる。これよりCAモジュール等の可搬による受信端末外部での契約も可能となる。よってCAモジュール等のユーザー個人特定蓄積媒体は持ち運びが可能となる。

【0015】また、受信端末で蓄積した暗号化コンテンツは、ユーザーの視聴時に暗号化されたコンテンツを複写し、同様に暗号化されたメタデータ1、2も複写し、複写したメタデータ1、2を復号化したのち、復号化したメタデータ1、2を使用することにより、複写されたコンテンツを復号化して再生する。これより暗号化されたコンテンツデータは常時蓄積された状態となり、いつでも別のCAモジュールで同様のサービスを楽しむことが可能である。

【0016】また、第3者に譲渡の目的でコンテンツを購入する際に、暗号化コンテンツと暗号化されたコンテンツに関する情報（メタデータ）と第3者に対する譲渡を目的にしていることを示すギフト情報で構成されたデータの組み合わせを行うことで譲渡目的としたサービスを行うことが可能となる。

【0017】

【発明の実施の形態】以下の見出しに従い説明する。

1. システム
2. データ構成
3. 暗号化・復号化
4. 受信端末
5. コンテンツ蓄積・視聴
6. 拡張サービス
7. まとめ

【0018】1. システム

（サービス概要）図1に、蓄積型テレビ放送サービスの受信側の概要図を示す。この受信側は、アンテナ2、受信端末3、テレビ17を備える。

【0019】本サービスの概要として、蓄積型テレビ放送について説明する。従来のテレビ放送は、放送サイド（放送局）から送られてくるコンテンツ1（番組）をアンテナ2（ケーブルでの伝送の場合もある）、受信端末3で受信し、テレビ17などのモニタ装置にて送られてきているその瞬間から視聴を行なう（ここでは、「リアルタイム型視聴6」と呼ぶ）。蓄積型テレビ放送とは、従来のテレビ放送と同様のリアルタイム型視聴6に加え、従来のビデオデッキなどと同様に一度送られてき

たコンテンツを蓄積媒体4（本発明ではこれを、例えば、HDDとして説明する）に蓄積後視聴する「蓄積型視聴8」、蓄積されたコンテンツと送られてきているリアルタイムのコンテンツを合わせて視聴する「リアルタイム型+蓄積型視聴7」などのサービスを可能とするテレビ放送である。なお、蓄積型視聴8では、DVDなどの可搬性に富んだリムーバブルメディア5を蓄積媒体として使用することもある。本発明では、上記のような蓄積型テレビ放送におけるサービス、特にコンテンツの暗号化、鍵の配信方式、契約方式などについて述べる。

【0020】（システム概要）蓄積型テレビ放送サービスを行なうシステムとしては、衛星放送、地上波放送など電波によるインフラのほかに、ケーブルテレビ、インターネットなどの通信線を利用したインフラでのサービスが可能である。本発明では、一例として、デジタル衛星放送、特にBSデジタル放送をインフラとした場合について述べる。

【0021】図2に、蓄積型テレビ放送サービスシステムの全体図を示す。まず蓄積型テレビ放送サービスが行なわれるシステムの全体を、この図を用いて説明する。

【0022】蓄積型テレビ放送サービスシステムは、コンテンツを制作、配信する放送サイドであるセンタ側9と、受信側である受信端末3（PDR: personal digital recorder以後受信端末を略してPDRと呼ぶ場合もある。）を備える。センタ側9では上記の通りコンテンツ及び関連した情報の制作、配信の他に著作権、視聴制御、課金などを考慮した暗号化、鍵管理、ユーザーリクエスト受け付けなども行なわれ、そのコンテンツ及び関連した情報を配信可能なデータへ組み立て、および、衛星10を介し受信端末3側に配信する。受信側である受信端末3は、衛星10を介したコンテンツ及び関連した情報をアンテナ2により受信し、TV17等のモニタ装置に直接出力、または蓄積媒体4内に蓄積後出力することで、ユーザーの視聴を可能とする。この受信端末3がTV17等のモニタ装置に内蔵されることもあるが、ここでは別装置として説明する。

【0023】蓄積型テレビ放送サービス用の受信端末3は、コンテンツ及び関連した情報を蓄積するための蓄積媒体4を有している他に、暗号/復号化モジュール200、CAモジュール1100、モジュール2101を備える。暗号/復号化モジュール200は、暗号化されて配信されたデータの復号化及び受信端末3内の重要なデータに対し暗号化を行ない、著作権保護等の権利、認証、課金などの処理、制御にかかわる。暗号/復号化モジュール200については、パイレーツや暗号解読などに対するセキュリティ対策として基本的に1デバイスにより構成されるが、さらなるセキュリティ対策として、モジュールごと取りかえることが可能な構成も考えられる。センタ側9と受信端末3を結ぶ地上回線18はコンテンツに対する課金処理、ユーザーの視聴履歴、リ

クエストの取得の他、コンテンツ、コンテンツに対する暗号化およびその他データに対する暗号化を解除するための情報、コンテンツに関連した情報、鍵の送信等を行なう場合などにも用いられる。

【0024】CAモジュール1100及びCAモジュール2101は、この受信端末3を使用するユーザーの個人認証、及びユーザーの属する家族などのグループの認証等を行う。ここでいうCAモジュール1100、モジュール2101には、メモリ媒体のほかBSデジタル放送で使用されるICカードを使用することもある。CAモジュール1100については、グループの認証や伝送路暗号の復号化機能等を有し、可搬性を考慮できないため受信端末3内にその機能を内蔵させることも可能となる。またCAモジュール2101は、個人認証機能等を持ち、可搬も可能であり、蓄積したコンテンツを外部機器11などで再生する際や外部機器11にてコンテンツの契約を行なう際に、リムーバブルメディア5と共に外部機器に接続し使用することもある。なお、CAモジュール1、2の各々の役割等については後述する。

【0025】2. データ構成

（コンテンツの定義）図3に、サービス、イベントの関係の説明図を示す。以下に、蓄積型テレビ放送サービスにおける前述したコンテンツ、及びそれに付随するイベント、サービスの単位について説明する。まずサービスとイベントの関係について説明する。

【0026】本蓄積型テレビ放送において、サービス35とは放送番組の連続をさし、従来のテレビ放送におけるチャンネルと同意であり、イベントとは上記サービス35（チャンネル）内で時間軸に対して1つ存在する放送番組をさす。例えば6:00~8:00の時間枠はイベントA36、8:00~9:00の時間枠はイベントB37、9:00~13:00の時間枠ではイベントC38となる。またサービス35（チャンネル）内のある任意の時間においてイベントが存在しない場合はあるが、2つ以上のイベントが存在することはない。さらにイベントとは、本蓄積型テレビ放送サービスにおいては複数コンテンツないしは単一のコンテンツにより構成される。

【0027】次に、図4に、イベント内のコンテンツ構成例の説明図を示す。以下に、コンテンツの構成およびそのコンテンツの単位について説明する。本蓄積型テレビ放送サービスにおいては、コンテンツとは放送サイドが意図する単位で自由に決められるものであり、それを構成する最小単位とはBSデジタル放送を例にするとリソースもしくはストリーム（PES）となる。

【0028】具体例として複数のストリーム、リソースにより構成されるイベント20の場合について説明する。イベント20は、映画配信22とデータ放送（例、料理）23により構成されるイベントである。コンテンツの構成としては、コンテンツA30~E34を有す

る。ここでは、コンテンツA30は、無料で見られるメインメニュー画面21を構成するBML文書などのリソース類を含む。コンテンツB31は、500円の視聴料が必要な映像ストリーム24や音声ストリーム25で構成される映画コンテンツである。コンテンツC32は、この映画コンテンツに対して追加料金200円を払うことにより視聴可能となる字幕データストリーム26である。コンテンツD33は、上記の視聴料とは別に視聴料300円が必要な複数リソースにより構成される料理メニュー27、中華レシピ28などの画面を含む料理コンテンツである。コンテンツE34は、その料理コンテンツ内で追加料金100円を払うことにより視聴可能となる単一リソースである隠し味テキスト29である。コンテンツを放送サイドが意図する課金単位と対応させて定義することにより、従来の放送番組すなわちイベント単位あるいはチャンネルであるサービス単位の課金とは異なり、上記イベント20のような最小課金単位が単一のストリーム（字幕データストリーム26）、単一のリソース（隠し味テキスト29）などの細かなコンテンツ単位課金、またそれらを組み合わせた複雑な課金を行なう放送番組を制作することが可能となる。またこのコンテンツの定義としては有料・無料の他に、著作権のあるなしなどによるコピー制御、視聴制御も含むことができる。これによりコンテンツ自体に暗号化を行なったまま蓄積媒体に保存することもある。

【0029】（メタデータの構成）次に、図5に、コンテンツに付随する情報の構成図を示す。以下に、上記コンテンツを配信するときに必要となる情報、配信されたコンテンツを蓄積する際に必要となる情報、そのコンテンツを検索するために必要な情報、視聴もしくは視聴契約を行なうために必要な情報、暗号化されたコンテンツを復号するための情報、さらにはコンテンツを外部機器に持ち出すときに必要となる情報等、コンテンツに対し付随する情報の構成等について説明する。

【0030】図において、蓄積型テレビ放送サービスを受信する受信端末（PDR）3内の蓄積媒体4、外部機器に持ち出す際に必要となるリムーバブルメディア5、前述した通り個人を認証する際や外部機器にコンテンツを持ち出す際に必要となるCAモジュール2101（ここではその物理的媒体を可搬性に富んだ「ICカード2」として説明する。）が示される。ICカード2は、受信端末3に登録されているユーザー数と同じだけの枚数が存在する、本例ではその登録ユーザー数をa、bの2ユーザーとし、ICカード2(a)用80、ICカード2(b)用81の2枚が存在するものとし説明する。蓄積型テレビ放送サービスでは、放送サイドはコンテンツに対し著作権、コピー制御、検索用の情報、視聴料などの課金に関する情報、配信するコンテンツが暗号化されている場合はその暗号を解除するための情報等（暗号化で使用された鍵、もしくは鍵のある場所や、その暗号方式を指定する情報

等）の様々な情報をコンテンツ1に対し添付して配信するが、そのようなコンテンツに関する情報を本発明では「メタデータ50」と呼ぶ。

【0031】受信端末（PDR）3では、配信されてきたコンテンツ1、メタデータ50をCAモジュール1100の契約情報等により随時蓄積媒体4に蓄積するか、もしくは復号化及び暗号化が必要であれば受信端末3内の暗号／復号化モジュール200にて処理など必要に応じて一部加工後、蓄積媒体4に蓄積する。さらにこの例では、メタデータ50は、配信されてきた状態では不完全な状態の場合もあり、別途配信されるBSデジタル放送ではPSI/SI（Program Specific Information/Service Information、番組特定情報/番組配列情報）と呼ばれる番組配列情報より必要な情報を取得し追記する場合もある。このメタデータ50は、メタデータA～Cを含み、例えば、メタデータA57のように少なくともコンテンツA56に対しひとつ配信され、蓄積媒体4内に蓄積される。また、前述したイベント20のような複雑なコンテンツ構成の場合、受信端末の検索、課金処理などを容易にするために、メタデータX58のように複数のコンテンツにまたがるようなメタデータX58を配信、蓄積することによりメタデータ50が階層化される場合もある。メタデータ152及び251、59は、例えば、コンテンツA56に対しひとつ存在するメタデータA57を元に、各ユーザーの視聴契約が行なわれる際に生成され、分新化される。また、複数ユーザーにより視聴契約が行なわれた場合には、メタデータ2A(a)51、メタデータ2A(b)59のように複数存在する。逆に視聴契約が行なわれない場合は存在しない場合もある。

【0032】メタデータ1A(a)52、メタデータ2A(a)51は、例えば、ユーザーが実際に蓄積されたコンテンツA56に対し視聴契約を行なった際に、メタデータA57にコンテンツA56が暗号化されている場合はそれに付随する情報、視聴契約の契約内容等の情報を追記し分割することにより生成される情報である。メタデータ1A(a)52は個人認証用のCAモジュール2101（本例ではユーザー(a)による視聴契約の場合であるためICカード2(a)用80）に埋め込まれ、メタデータ2A(a)51はコンテンツA56が蓄積されている蓄積媒体4内に保存される。またコンテンツA56を外部機器に持ち出すためにリムーバブルメディア5に移す、ないしはコピーする場合も、同じくそのコンテンツA56に伴うメタデータ2A(a)51をリムーバブルメディア5に書込む。メタデータ1A(a)52も同じくICカード2(a)用80に書込まれる。

【0033】受信端末3内部では、検索処理を向上させるために階層化されたメタデータに含まれる情報を吸い上げ、検索用テーブル55を生成する。この検索用テーブル55は、ユーザーが直接触れられるものではなく、ユーザーが検索などを行なう場合には、受信端末3内の

アプリケーションプログラムからプロファイル53、54を介し検索用テーブル55を利用し、該コンテンツの検索を行なう。この際使用可能なプロファイルを識別するためのパスワード入力などの個人認証が行なわれる。本蓄積型テレビ放送サービスにおけるプロファイルとは放送サイドより配信されるものではなく、予め受信端末3内に存在しユーザーの視聴契約情報すなわち蓄積媒体内のメタデータ2とCAモジュール2101内のメタデータ1より常に更新されるものである。このプロファイルには、個人契約にかかわるユーザー個人に対する個人用のプロファイル54と、各ユーザー間の相互関係などのグループ契約にかかわる全体プロファイル53が存在する。個人用プロファイルには受信端末3に登録されていないユーザーのためのゲスト用プロファイルも存在する。このプロファイル53、54と検索用テーブル55とのやりとりにより、ユーザーは蓄積媒体内に蓄積されているコンテンツに対してユーザー自身が利用可能なコンテンツの検索が可能となる。さらにプロファイルとしてはユーザーの視聴するコンテンツのジャンル等の履歴を保持し、それによりユーザー嗜好性に沿った自動コンテンツ蓄積などを実現する。以上が本蓄積型テレビ放送サービスにおけるコンテンツに付随する情報の構成である。

【0034】(配信データの構成)次に、図6に、配信時のデータ構成図を示す。以下に、コンテンツとそれに付随する情報を配信する際のデータ構成について説明する。

【0035】配信する際のデータ構成は、インフラとしてBSデジタル放送を利用する場合、データ放送コンテンツについてはDSM-CC伝送方式であるデータカルーセルにより伝送し、映像・音声・字幕などのストリームはPES伝送方式を利用する。以下に、前述したイベント20のコンテンツ構成の場合を例とし配信データの構成を説明する。本蓄積型テレビ放送サービスにおける配信時のデータ構成としては、デフォルトES060、映像・音声・データ・ストリームES161、ES262、ES363、データカルーセルES464、PSI/SI65等に分けられる。ES060は、受信端末3のデータ取得処理を向上させるためコンテンツの構成などの記載されたメタデータX58、メタデータA57などのメタデータを集め1つのESとしたデフォルトESである。ES1~461、62、63、64は、各種コンテンツを伝送するコンテンツ伝送用ESである。PSI/SI65は、これらのES群の構成、もしくはサービスの視聴契約、イベントの視聴契約、EPG生成用情報を含む。イベント20の場合、コンテンツB、コンテンツCのような映像ストリーム、音声ストリーム、データストリームといったPES伝送方式に依存するコンテンツはそれぞれ単体でES161、ES262、ES363、のようにESを構成する。一方データ放送コンテンツであるコンテンツA、コンテン

ツD、コンテンツEなどのカルーセル伝送方式に依存するコンテンツは、PESの場合と同様に単体でESを構成することも可能だが基本的にはデータ伝送効率を考慮し、ES464のように複数コンテンツによりESを構成し伝送される。またこの複数コンテンツにより構成されるESが複数ESとなる場合もある。

【0036】3. 暗号化・複号化

(暗号方式)本発明で示す総合データ配信サービスの暗号方式には著作権保護暗号方式と限定受信方式がある。

【0037】図23に、送信側において暗号化されたコンテンツ、メタデータの暗号形態の説明図を示す。まず、コンテンツ、メタデータの制作終了の時点で、コンテンツをファイルもしくはストリーム単位で著作権保護暗号で鍵Kk110を用いて暗号化する。その鍵をメタデータに埋め込み111メタデータファイルを著作権保護暗号で鍵Kwc112を用いて暗号化する。それら暗号化コンテンツ、暗号化メタデータの伝送形態であるMP EG-2 TSを鍵Ks113で暗号化する。

【0038】(コンテンツ暗号化方式)次に、図7に、蓄積型テレビ放送サービスにおける暗号化方式の説明図を示す。インフラであるBSデジタル放送の伝送路における伝送データ暗号化(Multi2暗号化方式)以外に、本発明では、コンテンツ自体に暗号化を行ない、暗号化したコンテンツを蓄積媒体に蓄積する。このような本発明で使用する本蓄積型テレビ放送サービス特有の暗号化方式(ここではK暗号と呼ぶ)について以下に、説明する。コンテンツ暗号方式は、伝送路の暗号化方式とは異なり、配信用データの組み立て後ではなくコンテンツの制作完了時に暗号化を行なう。コンテンツとは前述の通り放送サイドが意図する単位であるため、それを構成するリソース、ストリームなどの組み合わせも様々になる。よってここではその代表的な組み合わせを例に説明する。

【0039】例えば、コンテンツA30は、前述したイベント20のコンテンツAのように複数のBML文書などのリソースにより構成されるコンテンツである。コンテンツB31は、同様にイベント20におけるコンテンツBのように複数ストリームにより構成されるコンテンツである。コンテンツE34は、単一リソース、コンテンツC32は、単一ストリームで構成されるコンテンツである。コンテンツ暗号方式では、これら様々な構成によるコンテンツのいずれの場合も同様に暗号化を行うため、各リソース、ストリームを単に始まりと終わりのあるデータの塊としてとらえ、暗号化処理部70にてそれらのデータの塊を固定長ブロックに分け、ブロック毎に順番に暗号化を行なうものとする。この方式により、暗号化するデータのフォーマットであるリソース、ストリームの区別のない暗号化が可能となる。但し、暗号化処理部70より出力される暗号化された暗号化データ(リソース)71、暗号化データ(ストリーム)72は元の

データフォーマットであるリソース、ストリームの区別が出来なくなるため、生成される暗号化情報 7 3 は、例えば、別途その暗号化データ 7 1、7 2 の元のデータフォーマット、リソースの形式、各暗号化データ間の相互関係であるコンテンツ内の構成、暗号化を行なう際に使用した鍵、あるいは暗号方式を複数運用する場合は、掛けられている暗号方式の指定などの復号時に必要となる情報などを含む。放送サイドではこの暗号化情報 7 3 を元に暗号化データ（リソース）7 1 はカルーセル化、暗号化データ（ストリーム）7 2 は PES 化し、前述の配信データ構成のようなデータ構成に組み立てる。さらにこの暗号化情報 7 3 は番組配列情報である PSI/SI ないしはメタデータ 5 0 を生成する際にも反映される。またこのコンテンツに対する暗号化を行なう際に使用する鍵を本蓄積型テレビ放送サービスではコンテンツ鍵 Kk と呼ぶ。コンテンツ鍵 Kk は運用条件により 1 種類での運用、コンテンツ毎にユニークでの運用など様々な運用が可能である。

【0040】（鍵配信方式）まず、映像ストリームの伝送について説明する。一般に、映像ストリームは、固定長のデータにブロック化される。各ブロックにはヘッダ情報が追加される。TSP (Transport Stream Packet) は、このヘッダとデータの組であり、伝送時のデータパケットのフォーマットを指す。既存型でスクランブル（暗号）を掛ける場合はデータ部分を暗号化する。ECM (Entitlement Control Message) は、ユーザー全体に共通的に伝送される情報であり、番組情報および制御情報を含む共通情報の伝送メッセージである。番組情報とは、例えば、番組に関する情報とデスクランブルのための鍵などであり、制御情報とは、例えば、デコーダのデスクランブル機能の強制オン/オフの指令などである。ECM は、基本的にコンテンツのスクランブル鍵を伝送するため、コンテンツと共に伝送されるものであり、ある特定ユーザーに限定して送られる情報ではない。また、EMM (Entitlement Management Message) は、加入者毎の契約情報および共通情報の暗号を解くためのワーク鍵を含む個別情報の伝送メッセージである。EMM は、基本的にユーザーが契約した事業者の鍵等を送るため、ある特定ユーザーを限定して送られる情報である。また、CA (Conditional Access) system とは、限定受信方式を指し、サービス（編成チャンネル）やイベント（番組）の視聴を暗号化鍵で制御するシステムである。

【0041】次に、図 8 に、伝送路暗号とコンテンツ、メタデータ暗号の関係の説明図を示す。以下に、BS デジタル放送と本サービスにおける、暗号化データ及び鍵の配信方法について説明する。図には、BS 伝送路暗号 3 0 3 と、コンテンツ、メタデータ暗号 3 0 1、3 0 2 の関係が示される。コンテンツ、メタデータ暗号 3 0 1、3 0 2 はコンテンツ 1 やメタデータ 5 0 のデータを直接暗号化するのに対して、BS 伝送路暗号 3 0 3 はコンテン

ツ、メタデータ等を含んだイベントの伝送形態である TSP 3 0 0 に対して暗号化する。

【0042】（BS 伝送路暗号）図 9 に、伝送路における鍵配信方式の説明図を示す。以下に、BS 伝送路暗号 3 0 3 の暗号化データ及び鍵の伝送方法を説明する。まず、コンテンツ 1、メタデータ 5 0 等を含んだイベント 2 0 の伝送形態である TSP 3 0 0 に対して、スクランブル鍵 Ks 3 1 0 で暗号化 3 1 1 する。次にスクランブル鍵 Ks 3 1 0 をワーク鍵 Kw1 3 1 3 で暗号化 3 1 4 し、Ks' 3 1 5 を作成する。この時のワーク鍵 Kw1 3 1 3 は放送サイドの事業者毎に定めている鍵であって、本サービスの視聴可、不可に関わる鍵である。最後に、ワーク鍵 Kw1 3 1 3 を各受信端末（PDR）毎に一意である個人鍵 Km1 3 1 6 で暗号化 3 1 7 し、Kw1' 3 1 8 を作成する。これら、暗号化されたデータ及び鍵を、暗号化イベントデータ 3 1 2 は BS 伝送路、Ks' 3 1 5 は ECM 3 1 9、Kw1' 3 1 8 は EMM 3 2 0 を用いて伝送する。それら暗号化データを受信した受信端末（PDR）は CA モジュール 1 0 0 内に格納されている個人鍵 Km1 3 1 6 を用いて復号する。まず、EMM 3 2 0 で伝送された Kw1' 3 1 8 を個人鍵 Km1 3 1 6 を用いて復号 3 2 1 し、ワーク鍵 Kw1 3 1 3 を入手する。次に、ECM 3 1 9 を用いて伝送された Ks' 3 1 5 をワーク鍵 Kw1 3 1 3 を用いて復号 3 2 2 し、スクランブル鍵 Ks 3 1 0 を入手する。最後に、BS 伝送路を用いて伝送された暗号化イベントデータ 3 1 2 をスクランブル鍵 Ks 3 1 0 を用いて復号 3 2 3 し、イベントの伝送形態である TSP を入手する。

【0043】（コンテンツ、メタデータ暗号）以下に、コンテンツ鍵伝送モデルについて、ECM を用いた場合、及びメタデータを用いた場合の各々について説明する。

【0044】（ECM を用いたコンテンツ鍵伝送モデル）まず、コンテンツ鍵 Kk 3 3 0 を ECM 3 1 9 を用いて伝送する場合のコンテンツ 1、メタデータ 5 0 の伝送方法を説明する。

【0045】図 10 に、ECM を用いたコンテンツ鍵伝送モデルの説明図を示す。以下に、コンテンツ伝送について説明する。まず、コンテンツ 1 をコンテンツ鍵 Kk 3 3 0 で暗号化 3 3 1 する。次にコンテンツ鍵 Kk 3 3 0 をワーク鍵 Kw3 3 3 3 で暗号化 3 3 4 し、Kk' 3 3 5 を作成する。このワーク鍵 Kw3 3 3 3 は放送サイドの各事業者毎に定めている鍵である。この鍵は、BS 伝送路暗号で用いられる鍵 Kw1 3 1 3 を共用する事も可能である。最後に、ワーク鍵 Kw3 3 3 3 を各受信端末（PDR）もしくは受信端末（PDR）内の暗号/復号化モジュール毎に一意である鍵 Km3 3 3 6 で暗号化 3 3 7 し、Kw3' 3 3 8 を作成する。鍵 Km3 3 3 6 は全ての受信端末（PDR）において 1 種類にする事も可能である。これら、暗号化されたデータ及び鍵を、暗号化コンテンツは BS 伝送路、Kk' 3 3 5 は ECM 3 1 9、Kw3' 3 3 8 は EMM 3 2 0 を用いて伝送する。それら暗号化データを受信した受信端末（PDR）は

受信端末 (PDR) 内に格納されている鍵Kmc 3 3 6を用いて復号する。まず、EMM 3 2 0で伝送されたKwc' 3 3 8を鍵Kmc 3 3 6を用いて復号3 3 9し、ワーク鍵Kwc 3 3 3を入手する。鍵Kwc 3 3 3は一度受信端末 (PDR) に伝送されると更新されるまで受信端末 (PDR) 内に保持される。更新方法は、再度EMM 3 2 0を用いてKwc' 3 3 8を伝送し、Kmc 3 3 6を用いて復号3 3 9し、新しい鍵Kwc 3 3 3を入手する。次に、ECM 3 1 9を用いて伝送されたKk' 3 3 5をワーク鍵Kwc 3 3 3を用いて復号3 4 0し、コンテンツ鍵Kk 3 3 0を入手する。最後に、BS伝送路を用いて伝送された暗号化コンテンツ3 3 2をコンテンツ鍵Kk 3 3 0を用いて復号3 4 1し、コンテンツ1を入手する。

【0046】図11に、メタデータの伝送モデルの説明図を示す。以下に、メタデータ伝送について説明する。まず、メタデータ50をワーク鍵Kwc 3 3 3で暗号化350する。この時のワーク鍵Kwc 3 3 3はBS伝送路暗号で用いられる鍵Kwl 3 1 3を用いる事も可能である。次に、ワーク鍵Kwc 3 3 3を各受信端末 (PDR) 毎に一意である鍵Kmc 3 3 6で暗号化337し、Kwc' 3 3 8を作成する。これら、暗号化されたデータ及び鍵を、暗号化メタデータ351はBS伝送路、Kwc' 3 3 8はEMM 3 2 0を用いて伝送する。それら暗号化データを受信した受信端末 (PDR) は受信端末 (PDR) 内に格納されている鍵Kmc 3 3 6を用いて復号する。まず、EMM 3 2 0で伝送されたKwc' 3 3 8を鍵Kmc 3 3 6を用いて復号339し、ワーク鍵Kwc 3 3 3を入手する。次に、BS伝送路を用いて伝送された暗号化メタデータ351をワーク鍵Kwc 3 3 3を用いて復号352し、メタデータ50を入手する。

【0047】(メタデータを用いたコンテンツ鍵伝送モデル) 図12に、メタデータを用いたコンテンツ鍵伝送モデルの説明図を示す。以下に、コンテンツ鍵Kk 3 3 0をメタデータ50を用いて伝送する場合のコンテンツ1、メタデータ50の伝送方法を説明する。まず、コンテンツ1をコンテンツ鍵Kk 3 3 0で暗号化331する。そのコンテンツ鍵Kk 3 3 0をメタデータ50に追記し、メタデータ50をワーク鍵Kwc 3 3 3で暗号化350する。この時のワーク鍵Kwc 3 3 3はBS伝送路暗号で用いられる鍵Kwl 3 1 3を用いる事も可能である。最後に、ワーク鍵Kwc 3 3 3を各受信端末 (PDR) 毎に一意である鍵Kmc 3 3 6で暗号化337し、Kwc' 3 3 8を作成する。これら、暗号化されたデータ及び鍵を、暗号化コンテンツ332、暗号化メタデータ351はBS伝送路、Kwc' 3 3 8はEMM 3 2 0を用いて伝送する。それら暗号化データを受信した受信端末 (PDR) は受信端末 (PDR) 内に格納されている鍵Kmc 3 3 6を用いて復号する。まず、EMM 3 2 0で伝送されたKwc' 3 3 8を鍵Kmc 3 3 6を用いて復号339し、ワーク鍵Kwc 3 3 3を入手する。次に、BS伝送路を用いて伝送された暗号化メタデータ351をワーク鍵Kwc 3 3 3を用いて復号352し、メタ

データ50を入手する。最後に、BS伝送路を用いて伝送された暗号化コンテンツ332をメタデータ50に記入されているコンテンツ鍵Kk 3 3 0を用いて復号し、コンテンツ1を入手する。

【0048】(拡張モデル) 上記の2つのモデルにおいては、コンテンツ鍵Kk 3 3 0はコンテンツとセットで伝送している。それ以外に、拡張モデルとして、上記2つのモデルでコンテンツ鍵Kk 3 3 0を伝送しているECM 3 1 9またはメタデータ50では、コンテンツ鍵Kk 3 3 0を記入せずに、コンテンツ鍵Kk 3 3 0の所在を示すURL、鍵ID等の情報のみを記入し、コンテンツとセットで伝送することも可能である。その際のコンテンツ鍵Kk 3 3 0の所在として、鍵管理センタ、受信端末 (PDR) 内RAM、HDD等が想定される。鍵入手方法として、地上回線、衛星回線等を用いて鍵管理センタから鍵を入手する方法や、前もって地上回線、衛星回線等を用いて受信端末 (PDR) 内のRAMに対して全ての鍵を配信しておき、必要に応じて鍵を入手する方法や、地上回線、衛星回線等を用いて、コンテンツ1、メタデータ50とは別に、鍵ファイルとして配信してHDDに蓄積し、必要に応じて入手する方法が可能である。

【0049】(鍵管理) ECM 3 1 9を用いたコンテンツ鍵伝送モデル、メタデータ50を用いたコンテンツ鍵伝送モデルのどちらも、受信端末 (PDR) 内ではコンテンツ鍵Kk 3 3 0はコンテンツとセットであるメタデータに記入されている。よって、コンテンツ鍵Kk 3 3 0はコンテンツ1毎に変更可能である。つまり、全てのコンテンツ1を1つの鍵で管理したり、全てのコンテンツ1に異なる鍵を用いる事もでき、幅広い鍵管理方法が可能である。

【0050】4. 受信端末

(受信端末の構成) 図13に、受信端末の構成図を示す。次に本蓄積型テレビ放送サービスを受信するのに必要な受信端末3内の構成を説明する。受信端末3は、アンテナ2を介しコンテンツ・メタデータ・番組配列情報PSI/SIなどの各種データを受信する受信モジュール12、受信したコンテンツなどのデータを蓄積する蓄積媒体4、リムーバブルメディア5とのI/Fであるリムーバブルメディア用ドライブ16、契約情報等の個人ないしはグループの情報が書き込まれているCAモジュール1100及びCAモジュール2101、コンテンツをTV17等のモニタ装置で表示・再生させるためのデコーダ15、暗号/復号化モジュール200、各処理にかかわるCPU13、メモリ14を備える。リムーバブルメディア5は、蓄積したコンテンツを外部機器で使用するために必要なものである。

【0051】受信モジュール12は、受信したデータの中でユーザーが選択したサービスに必要なデータのみを抽出する機能や、CAモジュール1100を利用することにより前述した伝送路におけるBS暗号方式である

Mulli2暗号を解除するデスクランブル機能を持つ。蓄積媒体4ないしリムーバブルメディア5に受信モジュール12で受信したコンテンツを蓄積する際のコンテンツの蓄積形態は、上記の伝送路の暗号が解かれた形態で蓄積される。そのため、蓄積されるコンテンツ1は、本蓄積型テレビ放送サービス用の暗号が掛けられた暗号あり、リソース39、暗号ありストリーム41、暗号化がされていない暗号なしリソース40、暗号なしストリーム42の組み合わせにより構成される。一方蓄積媒体4にコンテンツと共に蓄積されるメタデータは、伝送時の暗号を暗号/復号化モジュール200にて一度復号し、その後再び暗号/復号化モジュール200内で生成もしくは用意される使い捨て鍵KIにより暗号化され蓄積媒体4に蓄積される。

【0052】さらに、暗号/復号化モジュール200は、受信端末3内でのデータの暗号化、復号化、その他権利、認証、課金等の処理、制御に関わる。詳細には、暗号/復号化モジュール200では、ユーザーの視聴契約の際に蓄積媒体4内に蓄積されたメタデータ(KIで暗号化されている)を復号し、メタデータ1、2を生成する機能、使い捨て鍵KI'にて再び暗号化を行ない、蓄積媒体4内にメタデータ2を、CAモジュール2にメタデータ1と共に鍵KI'もしくは鍵に関する情報を伝送する機能を持つ。この際に使用される暗号化方式はコンテンツに対する暗号化方式とは異なるため、使い捨て鍵KI、KI'はコンテンツに対して使用した鍵Kkと同じものを使用することも可能である。暗号/復号化モジュール200は、暗号化、復号化、使い捨て鍵の生成、使い捨て鍵KIの鍵情報の保持(不揮発性メモリ等)、鍵管理、受信端末(PDR)3内で認証が必要となる各種データの、ユーザーへの認証、著作権保護、又は課金等に関する処理、制御機能を有する。さらに、暗号/復号化モジュール200は、蓄積媒体4、リムーバブルメディア用ドライブ16、リムーバブルメディア5、CAモジュール1、2100、101、地上回線18、IEEE1394など外部につながる外部I/F19などのI/Fに対しての伝送路のセキュリティ保護及びこれら伝送路を用いてメタデータ等の守るべきデータの伝送の際に伝送路やデータに合わせた暗号化を行ない、セキュリティ方式を選択する機能をも有する。

【0053】(CAモジュールの役割及び契約方式)本サービスでは、CAモジュールを2種類用意する。これより、個人単位のサービス提供及び課金等が可能である。CAモジュールとしては、ICカードやスマートメディア等が考えられる。CAモジュール1100は、主に、受信端末3に装着・内蔵することができ、CAモジュール2101とは異なり可搬性の必要でないものであり、グループ契約情報、伝送路の暗号を解くための鍵情報等の情報をもつ。CAモジュール2101は、リムーバブルメディアと共に受信端末外に持ち出すため可搬性の必要

な、個別契約情報、使い捨て鍵の情報等をもつ。また、暗号化コンテンツ、それに伴うメタデータをメタデータ1、2に分散化し蓄積することにより、本蓄積型テレビ放送サービスではバイレーツ、著作権侵害、不正コピーなどに対するセキュリティを高めている。

【0054】(CAモジュール1の役割及び契約方式)CAモジュール1は各受信端末(PDR)に1ずつ用意され、可搬性を持たず、受信端末(PDR)内に常時装備される。CAモジュール1は、その特性上常に受信端末(PDR)内に保持され得るので、受信端末(PDR)と分離可能な形態であるICカード等の記録媒体以外にも、受信端末(PDR)内蔵RAM等にその機能を持たせることも可能である。また、視聴権利単位は1台の受信端末(PDR)、つまり1個のCAモジュール1に対して、家族・グループ単位とすることができる。支払対象者の単位は、受信端末(PDR)、つまり1個のCAモジュール単位1とすることができる。なお、課金対象物の単位は、各チャンネルであるサービス単位、放送番組であるイベント単位である。スクランブルがかかったサービスないしイベントはCAモジュール1の情報により、視聴可否を判別する。また、コンテンツの視聴契約方法は、事前契約等が考えられる。つまり、前もって放送サイドの事業者に対し契約意思を表示しておく必要がある。

【0055】(CAモジュール2の役割及び契約方式)CAモジュール2は、契約した各個人に対し1ずつ用意され、可搬性を持たせている。その視聴契約単位はひとつのCAモジュール2に対して、個人単位となる。よって支払対象者の単位は個人単位とすることができる。しかし、チャンネルによってはグループ契約を設けることも考えられ、その際はグループとして登録した視聴者単位での視聴契約と課金が可能である。なお、課金対象物の単位は、各コンテンツ単位である。その際のコンテンツの最小単位は前述のとおりリソースもしくはストリームである。つまり、最小でリソース単位、ストリーム単位での課金が可能である。コンテンツの視聴契約方法は、事前契約、予約録画時契約、リアルタイム録画時契約、蓄積後視聴時契約等がある。

【0056】5. コンテンツ蓄積・視聴

(課金処理)コンテンツ蓄積は課金処理と関連するので、まず課金処理について概説する。有料コンテンツに対して、視聴契約を行うと課金処理が行われる。課金処理はメタデータに記載されている課金情報と、ユーザーが視聴契約の際に選択、追記した、視聴期間、視聴回数等の視聴条件等の情報を基に処理が行われる。課金処理が行われると、課金処理情報が受信端末(PDR)内の履歴を保持するためのメモリと、視聴契約したコンテンツとセットのメタデータに追加で書込まれる。

【0057】課金処理が行われるタイミングは視聴契約方法によって異なる。そのタイミングとしては、例えば、蓄積前課金処理、蓄積時課金処理、蓄積後課金処理

等がある。まず、蓄積前課金処理では、コンテンツ、メタデータがHDDに蓄積される前に課金処理が行われ、課金処理が行われないと蓄積する事ができない。つまり、コンテンツが配信される前に視聴契約が行われる時である。コンテンツの視聴契約方法として、事前契約、予約録画時契約等が想定される。また、蓄積時課金処理では、コンテンツ、メタデータがHDDに蓄積される時に課金処理が行われる。つまり、コンテンツが配信されていて、そのコンテンツを蓄積する際に視聴契約が行われる時である。コンテンツの視聴契約方法として、リアルタイム録画時契約等が想定される。また、蓄積後課金処理では、コンテンツ、メタデータがHDDに蓄積された後に課金処理が行われる。つまり、HDDに蓄積されているコンテンツに対して視聴契約が行われる時である。コンテンツの視聴契約方法として蓄積後視聴時契約等が想定される。

【0058】(コンテンツ蓄積(HDD))ここでは、配信されたコンテンツ1、メタデータ50を受信端末(PDR)3内HDD4又はリムーバブルメディア5に蓄積するまでの処理を説明する。なお、蓄積の際にも暗号化がなされる。ここでは、本蓄積型テレビ放送サービスにおいて、課金処理として蓄積後課金をサービスとした例として示す。なお、コンテンツ蓄積は、以下のようなECMを用いた蓄積とメタデータを用いた蓄積のうち、システム上いずれか一方の方式を採用することができる。また、両方の蓄積方法を使うことが可能なように設定することもできる。

【0059】「(a)ECMを用いた蓄積」と「(b)メタデータを用いた蓄積」の違いは、コンテンツの鍵Kkの配信方法が異なるという点のみである。すなわち、「(a)ECMを用いた蓄積」ではECMを用いて配信するのに対し、「(b)メタデータを用いた蓄積」では配信時からメタデータに格納して配信する。しかも、「(a)ECMを用いた蓄積」の場合には、後述するようにメタデータにコンテンツの鍵Kkの格納処理を行うので、HDDに蓄積する際は、「(a)ECMを用いた蓄積」と「(b)メタデータを用いた蓄積」は全く同じ形態となる。よって、それ以降の「コンテンツ視聴」における処理手順は全く同じとなる。一方、「(c)リムーバブルメディアに蓄積」は、「(a)ECMを用いた蓄積」「(b)メタデータを用いた蓄積」のどちらかの方式を用いてHDDに蓄積されたコンテンツとメタデータを、契約手続きと課金処理終了後にリムーバブルメディアに改めて蓄積する場合である。よって、その後の「コンテンツ視聴」処理は、「(a)ECMを用いた蓄積」又は「(b)メタデータを用いた蓄積」の後の視聴の場合とは異なる。

【0060】(a. ECMを用いたコンテンツ鍵伝送モデルにおける蓄積)図14に、ECMを用いたコンテンツ鍵伝送方式における処理手順の説明図を示す。また、図16に、コンテンツ鍵伝送方式における処理手順1のフロー

チャートを示す。以下に、ECMを用いたコンテンツ鍵伝送方式における処理手順を説明する。なお、この処理は、主に、暗号/復号化モジュール200により実行される。また各鍵については、図9～図12中の記号を示す。

【0061】まず初めにKs310、Kw1313とCAモジュール1100に蓄積されているKm1316を用いて、BS伝送路スクランブルを復号し(500)、暗号化コンテンツ401、暗号化メタデータ402を入手する。次に、予め受信端末(PDR)3に伝送され暗号/復号化モジュール200のRAM403に蓄積されているワーク鍵Kwc333を用いて、ECM400(319)を用いて伝送されたKk'335を復号し(501)、コンテンツ鍵Kk330を入手し(502)、RAM403に格納する。その後、暗号/復号化モジュール200のRAM403に格納されているワーク鍵Kwc333を用いてメタデータ402を復号し(503,404)、メタデータに記載されている検索/課金などの検索処理に用いられる情報を抽出し検索テーブル410に追加する(504)。この検索テーブル410はHDD4内のコンテンツ406の検索/課金情報などが記載されていて、検索をする際に使用される。メタデータから検索処理に用いられる情報を抽出し検索テーブルに追記した後、メタデータ402にコンテンツ鍵Kk330を追記する(505,404)。さらに、受信端末(PDR)3内の暗号/復号化モジュール200で生成もしくは用意させた値K1404を鍵K1として(506)、Kwcで一度復号されたメタデータをK1で再暗号化404し(507)、K1で暗号化されたメタデータ405を生成する404。鍵K1は暗号/復号化モジュール200のRAM403に格納される。この鍵K1は、メタデータ402をHDD4蓄積前に復号し再暗号化404する度に暗号/復号化モジュール200内で生成もしくは用意させる鍵である。その後、コンテンツ鍵Kk330で暗号化された暗号化コンテンツ406と鍵K1で暗号化された暗号化メタデータ405をセットでHDD4に蓄積する(508)。なお、メタデータ405毎に異なる鍵としてもよい。

【0062】(b. メタデータを用いたコンテンツ鍵伝送モデルにおける蓄積)図15に、メタデータを用いたコンテンツ鍵伝送方式における処理手順の説明図を示す。また、図17に、コンテンツ鍵伝送方式における処理手順2のフローチャートを示す。以下に、メタデータ50を用いたコンテンツ鍵伝送方式における処理手順を説明する。

【0063】まず初めにKs310、Kw1313とCAモジュール1100に蓄積されているKm1316を用いてBS伝送路スクランブルを復号し(500)、暗号化コンテンツ401、暗号化メタデータ451を入手する。この場合、暗号化メタデータ451には、コンテンツ鍵Kkが含まれる。次に、予め受信端末(PDR)3に伝送され

暗号/復号化モジュール200内のRAM452に格納されているワーク鍵Kwc333を用いてメタデータ451を復号し(503、453)、メタデータに記載されている検索/課金情報などの検索処理に用いられる情報を抽出し検索テーブル410に追加する(504)。この検索テーブル410はHDD4内のコンテンツ406の検索/課金情報が記載されていて、検索をする際に使用される。メタデータから検索処理に用いられる情報を抽出し検索テーブルに追記した後、暗号/復号化モジュール200内で生成もしくは用意させた値Kiを鍵Ki453として(506)、Kwcで一度復号されたメタデータをKiで再暗号化453し(507)、Kiで暗号化されたメタデータ405を生成する(453)。鍵Kiは暗号/復号化モジュール200内のRAM452に格納される。この鍵Kiは、メタデータ451をHDD4蓄積前に復号し再暗号化453する度に暗号/復号化モジュール200内で生成もしくは用意させる鍵である。その後、コンテンツ鍵Kk330で暗号化された暗号化コンテンツ406と鍵Kiで暗号化された暗号化メタデータ405をセットでHDD4に蓄積する(508)。なお、メタデータ414毎に異なる鍵としてもよい。

【0064】(c. リムーバブルメディアへのコンテンツ蓄積) 図18に、リムーバブルメディアへのコンテンツ蓄積処理手順のフローチャートを示す。以下に、HDD4に蓄積されたコンテンツ406をリムーバブルメディア5に蓄積するまでの処理手順を説明する。図14、図15にリムーバブルメディアへのコンテンツ蓄積処理の説明図を示す(両者は同様である)。

【0065】ユーザーがキーワード等を入力することにより、検索テーブル410の情報を基にHDD4内の検索処理412が行われる(520)。その検索結果より、ユーザーが蓄積コンテンツ409を選択する(520)。そして、選択されたコンテンツ409に対するメタデータ408を受信端末(PDR)3内のワークエリアにコピーする。コピーされたメタデータ408を鍵Kiを用いて復号413する(522)。そして、ユーザーが、選択したコンテンツ408の契約条件を確認後必要な情報を追記し、蓄積を決定415する(523)。ユーザーの蓄積決定の動作を受けて、ユーザーが契約した契約条件より課金処理416が行われる(524)。契約条件、課金処理の結果より、メタデータ414の契約情報を作成する(525)。その後、メタデータ414をメタデータ1、2に分離する(526)。そして、受信端末(PDR)3内で生成もしくは用意させた値Ki'を鍵Ki'418とする(527)。この鍵Ki'は、コンテンツ409の視聴手続き後、メタデータ2をリムーバブルメディア5、HDD4等に蓄積前に暗号化する度に受信端末(PDR)3内で生成もしくは用意させる鍵である。メタデータ2を鍵Ki'で暗号化し(528)、リムーバブルメディア5に蓄積する(529)。次に、メタデータ1

に鍵Ki'もしくは、鍵に関する情報を記入する。メタデータ1をセキュリティが守られている伝送路を用いてCAモジュール2101に蓄積し(531)、CAモジュール2101に蓄積されている個人鍵Km2424を用いて暗号化422する(530)。この処理において、セキュリティが守られている伝送路を用いて個人鍵Km2424を受信端末(PDR)3内に入力し、鍵Ki'もしくは鍵Ki'に関する情報を含んでいるメタデータ1を個人鍵Km2424を用いて暗号化した(422、530)後、CAモジュール2101に蓄積する(531)事も可能である。またこれ以外の方法として、セキュリティが守られた伝送路で鍵Ki'もしくは鍵Ki'に関する情報を含んでいるメタデータ1をCAモジュール2101に伝送し、そのまま保存する場合もある。メタデータ414に関する処理が全て完了したら、暗号化コンテンツ409をリムーバブルメディア5に蓄積する(532)。

【0066】このようにして、リムーバブルメディアに格納される情報は、鍵Kk'で暗号化され鍵Kkを含むメタデータ2421、鍵Kkで暗号化されたコンテンツ427となる。

【0067】(コンテンツ視聴) 図19に、コンテンツ視聴処理手順のフローチャートを示す。また、図24に、ECM又はメタデータを用いた蓄積後視聴のデータの流れについての説明図を示す。以下に、図14(図15)を参照して、HDD4に蓄積されたコンテンツ408を視聴するまでの処理手順を説明する。

【0068】HDD4には、鍵Kkを含む暗号にメタデータと暗号化コンテンツが記帳されている。ユーザーがキーワード等を入力することにより、検索テーブル410の情報を基にHDD4内の検索処理412が行われる(520)。その検索結果より、ユーザーが視聴コンテンツ409を選択する(540)。そして、選択されたコンテンツ409に対するメタデータ408を受信端末(PDR)3内のワークエリアにコピーする。

【0069】メタデータについては、次のように処理される。コピーされたメタデータ408を鍵Kiを用いて復号413する(522)。そして、ユーザーが、選択したコンテンツ409の契約条件を確認後、視聴を決定415する(541)。ユーザーの視聴決定の動作を受けて、ユーザーが確認、契約した契約条件より課金処理416が行われる(524)。契約条件、課金処理の結果より、メタデータの契約情報を作成417する(525)。その後、メタデータ414をメタデータ1、2に分離する(526)。そして、受信端末(PDR)3内で生成もしくは用意させた値Ki'を鍵Ki'とする(527)。この鍵Ki'は、コンテンツ409の視聴手続き後、メタデータ414をリムーバブルメディア5、HDD4等に蓄積する前に暗号化する度に受信端末(PDR)3内で生成もしくは用意させる鍵である(なお、メタデータ414毎に異なる鍵としてもよい)。次に、メタデー

データ2を鍵K1'で暗号化419し(528)、HDDに蓄積する(542)。次に、セキュリティが守られている伝送路を用いて個人鍵Km2 424を受信端末(PDR)3内に入力し、鍵K1'もしくは鍵K1'に関する情報を含むメタデータ1を個人鍵Km2 424を用いて暗号化422した(530)後、CAモジュール2 101に蓄積する(531)。この処理において、メタデータ1に鍵K1'もしくは鍵K1'に関する情報を記入する。メタデータ1をセキュリティが守られている伝送路を用いてCAモジュール2 101に蓄積し(531)、CAモジュール2 101に蓄積されている個人鍵Km2 424を用いて暗号化422する(530)。またこれ以外の方法として、セキュリティが守られた伝送路で鍵K1'もしくは鍵K1'に関する情報を含むメタデータ1をCAモジュール2 101に伝送し、そのまま保存する場合もある。一方、コンテンツについては、次のように処理される。メタデータ414に関する処理が全て完了したら、コンテンツ鍵Kk330を用いて暗号化コンテンツ409を復号426し(543)、視聴可能なコンテンツを入手する。

【0070】つぎに、図25に、リムーバブルメディアに蓄積後視聴のデータの流れについての説明図を示す。リムーバブルメディア5からの視聴処理についてもこのHDD4からのコンテンツの視聴処理と同様な処理が行われる。ただし、ここでは、CAモジュール2 101に蓄積されたメタデータ1と、リムーバブルメディア5の蓄積されたメタデータ2との一致確認及び契約条件確認が行われた後、コンテンツの視聴(復号)が可能となる。暗号化メタデータ1は、セキュリティが守られている伝送路を用いて個人鍵Km2 424を受信端末3内に入力し復号することができる。復号化されたメタデータ1内の鍵K1'を用いて、暗号化メタデータ2が復号化されることができる。メタデータ2内に格納されているコンテンツ鍵Kkにより、暗号化コンテンツを復号し、視聴可能となる。

【0071】6. 拡張サービス

次に本蓄積型テレビ放送サービスにおいてリムーバブルメディアを利用したサービス(コンテンツの外部での使用)の拡張サービスとしての第3者への譲渡を目的としたギフトサービスについて、概要を説明する。

【0072】図20に、通常サービスの説明図を示す。これは、前述したとおり、ユーザー600が視聴契約を行なったコンテンツを、視聴契約を行なった受信端末(PDR)3の外部で利用する場合である。受信端末(PDR)3から持ち出す形態は、メタデータ1の書込まれたCAモジュール2 101と、メタデータ2及び暗号化コンテンツが書込まれたリムーバブルメディア5である。通常サービスでは、外部受信端末(PDR)604、もしくは外部機器11で利用する場合にその両者を挿入あるいは接続し、ユーザー600の持つ視聴契約の権利(個人認証など)、すなわちCAモジュール2 101のメタ

データ1、リムーバブルメディア5のメタデータ2に基づきコンテンツの視聴が可能となる。

【0073】図21に、ギフトサービスの説明図を示す。ギフトサービスでは、ユーザー600である送り主601が、ギフト目的の視聴契約を行なった際に生成されるメタデータのみに基づくのではなく、受け取り主602側でコンテンツに対する認証およびその他必要な情報が視聴契約の際にリムーバブルメディア5に書込まれ、その後視聴可能となる。この場合送り主601側の受信端末(PDR)3では送り主のCAモジュール2 101で一度視聴契約を行ない、その際に生成されたメタデータに対し必要な部分に暗号化を行ないコンテンツの書き込まれたリムーバブルメディア5に書き込み受け渡す。一方、受け取り主602側の受信端末(PDR)604では、暗号化メタデータを復号し、受け取り主のCAモジュール2 604を使用し必要な視聴契約を行ない初めてコンテンツの視聴に必要なメタデータ1、2が生成され、コンテンツの視聴が可能となる。そのため個人の認証機能を持つCAモジュール2(送り主側の)をコンテンツと共に受け渡す必要がなくなる。この際にコンテンツなどの受け渡しの伝送路603は、リムーバブルメディアなどの蓄積媒体を介す手渡しや配送などのほかに、コンテンツなどのデータを放送波などの電波、地上回線などの通信線を利用し受け渡すことも可能である。

【0074】また、メタデータに対する暗号化は通常サービスと同様に暗号/復号化モジュール内で行なわれ、その際に使用される鍵は暗号/復号化モジュールで生成もしくは用意されたものを使用する。この際に使用する鍵をギフト鍵と呼ぶ。ギフト鍵は通常サービスと同様に生成もしくは用意された鍵K1、K1'を使用することも可能である。

【0075】図22に、ギフトサービスの伝送路において必要な情報の説明図を示す。以下に、リムーバブルメディアに書込む場合を例に、ギフトサービスを行なう際のコンテンツの受け渡しに必要な情報を説明する。コンテンツ607は、前述の通常サービスと同様に暗号化されたコンテンツである。メタデータ606は、送り主側で行なわれた視聴契約により作成されたメタデータの暗号化された部分であり暗号化されたコンテンツ607を復号するための鍵Kkもしくは鍵に関する情報、検索/課金情報などを含んでいる。ギフト情報605は、メタデータの暗号化されていない部分であり、通常サービスとギフトサービスを識別する情報、暗号化したメタデータを復号するための情報等を含む情報である。この情報を本例ではギフト情報と呼ぶ。メタデータ606については受け取り主側でコンテンツ607を視聴する前に受け取り主のCAモジュール2 604を基に必要な視聴契約処理を行なうことにより前述のメタデータ1、2となる。またこれ以外の方法としてメタデータを復号するための情報、ギフト情報、メタデータの一部などは、通常

サービスにおけるCAモジュール2内に分離したメタデータ1と同様に分離させ、別のセキュリティの守られた伝送路、例えば地上回線、センタ側などを利用し受け取り主側に受け渡すことも可能である。

【0076】7. まとめ

本発明の特徴のいくつかを以下に例示する。

- ・第3者に譲渡の目的でコンテンツを購入する際に、暗号化コンテンツと暗号化されたコンテンツに関する情報（メタデータ）と第3者に対する譲渡を目的にしていることを示すギフト情報で構成されたデータの組み合わせで譲渡目的としたサービスを実現可能とするシステムを提供すること。

- ・前記システムにおいて、暗号化されたコンテンツに関する情報（メタデータ）は、コンテンツの暗号化の鍵とは異なる鍵を用いて暗号化されていること可能とすること。

- ・前記システムにおいて、コンテンツに関する情報（メタデータ）にかかる暗号化のアルゴリズムとコンテンツにかかるアルゴリズムが異なること。

【0077】・前記システムにおいて暗号化のアルゴリズムを2種類用いることで、コンテンツに関する情報（メタデータ）とコンテンツの暗号化に用いる鍵は同じ鍵を用いることも可能であり、また異なる鍵を用いることも可能となること。

- ・前記システムにおいて、ギフト情報内にコンテンツに関する情報（メタデータ）を暗号化している鍵に関する情報を含むこと。

- ・前記システムにおいて、コンテンツに関する情報（メタデータ）には、受け取り側の所持する個人認証情報、CAモジュール2に通常格納される状態の情報は記入されてなく、譲渡目的の形式であるコンテンツセットを受け取ったときに、受け取り側である所有者が認識されるので、コンテンツに関する情報（メタデータ）に受け取り側を認識できる情報が初めて記入され、通常の情報形式になること。

【0078】・受信端末における暗号化コンテンツに対する管理を行う機能では、暗号化コンテンツの著作権管理、コンテンツに関する情報（メタデータ）の暗号／復号化、守るべきコンテンツに関するデータ、守るべき情報の移動に使用する伝送路に合わせた暗号化を行い、セキュリティ方式の選択を可能とすること。

- ・コンテンツはコンテンツ暗号鍵K_kで暗号化し、コンテンツに関する情報であるメタデータはコンテンツとは別の鍵で同様に暗号化を行い、この二つのデータの組み合わせによる構成でコンテンツに関する視聴・購入を行わせること。

- ・前記暗号化されたコンテンツとコンテンツに関するメタデータは衛星回線を介して衛星回線の伝送用暗号方式でさらに暗号化された後伝送されること。

【0079】・前記コンテンツ毎にユニークな鍵ないし

は同一の鍵で暗号化を行い、暗号化の鍵情報（鍵の存在場所や鍵そのもの）をメタデータに埋め込んで配信すること。

- ・前記暗号化されたコンテンツの鍵を、メタデータと同一の鍵で暗号化してコンテンツ配信時とは別の時間帯や、別の配信場所で配信すること。

- ・衛星デジタル放送におけるCAモジュールに対して個人を特定可能とする第2のCAモジュールを有し、この第2のCAモジュールがユーザー個人認証の役割を行うことでマルチユーザー対応とすること。

- ・受信端末内に暗号・復号化を行う専用モジュールを有し、この専用モジュールは暗号化されているメタデータを受信後直に伝送依存する鍵で復号化を行い、受信端末内で生成される使い捨て鍵で再度暗号化を行い受信端末にメタデータを蓄積させること。

【0080】・ユーザーの視聴・契約の動作に伴い、前記蓄積されている暗号化メタデータを復号し必要なデータを記入後再度新規使い捨て鍵の生成を行い、新規使い捨て鍵でメタデータを暗号化し、この暗号化メタデータを受信端末内に蓄積する、このようにユーザーのコンテンツ視聴・契約毎に新規使い捨て鍵を生成し、同じコンテンツであっても異なる使い捨て鍵となること。

- ・前記生成された新規使い捨て鍵を、受信端末と第2のCAモジュール間のセキュリティ保護された伝送インタフェースを通して、第2のCAモジュールに格納すること。

- ・受信端末内の暗号／復号化モジュールにおいて、モジュールそのものがモジュール特定鍵K_{mc}を有し、コンテンツ暗号鍵やメタデータの伝送時暗号に用いる伝送路鍵をモジュール特定鍵で暗号化し、受信端末内の暗号／復号化モジュールにデジタル放送の伝送方式を用いて配信し、暗号・復号モジュールで伝送路鍵を取得しモジュール内に格納後、伝送路鍵の更新において再度取得しモジュール内に格納する暗号／復号化モジュールを有すること。

【0081】・暗号化されたコンテンツを格納するときは、暗号化されたままの状態に格納し、暗号化されたコンテンツのメタデータも一緒に格納され、コンテンツの購入時にコンテンツ購入に関するデータをメタデータに記入し、メタデータはメタデータ1とメタデータ2とに分かれ、夫々のメタデータが暗号化された後、コンテンツ鍵で暗号化されたコンテンツと購入時に暗号化されたメタデータ2が受信端末内に2つセットで格納され、同様に暗号化されたメタデータ1はCAモジュール2に記録され、コンテンツ視聴時に分割されたメタデータを組み立てることで暗号化されたコンテンツの復号を可能とすること。

- ・コンテンツを暗号化しているコンテンツ鍵K_kは、本システムで管理する伝送路鍵K_{wc}で暗号化されてコンテンツ鍵K_{k'}となり、さらに伝送路鍵K_{wc}を暗号／

復号化モジュールの鍵 K_{mc} で暗号化し k_{wc} を作成、その後伝送路にて $K_{k'}$ 、 K_{wc} を送信しモジュール特定鍵 K_{mc} で解読して伝送路鍵 K_{wc} を取得する方式において、暗号/復号化モジュール内で伝送路鍵 K_{wc} を格納し、受信後の蓄積時とユーザー契約時に受信端末内で使い捨て鍵を生成、その使い捨て鍵と契約関連情報等、さらにデジタル放送の番組配列情報よりの組み合わせで作成すること。

・上記システムにおいて、暗号化されたコンテンツ購入時に作成されるメタデータの分割時における、暗号化されたコンテンツと一緒に蓄積させるメタデータ2は、装置内で生成される使い捨て鍵で暗号化され、残りのメタデータ1はコンテンツ鍵を書込み後同様に使い捨て鍵で暗号化して、暗号化されたコンテンツ、メタデータをリムーバブルメディアに記録すること。

【0082】・コンテンツ個々に対する暗号化並びに課金管理を行うことが可能となる上記システムにおいて、コンテンツ毎に異なる暗号鍵を所有することで様々な伝送路よりのコンテンツ組み合わせを可能とすること。

・家庭内受信端末では受信した暗号化コンテンツと一緒に配信されてきたメタデータと同時に格納し、家庭内における受信装置ではユーザーの購入時に受信したメタデータを元に有効期限等埋め込まれたメタデータの作成を行い、そのメタデータからメタデータ1、メタデータ2を作成しメタデータを受信端末で作成する使い捨て鍵を用いて暗号化し再度受信端末内に蓄積し、メタデータはユーザー特定の個人鍵 K_{m2} で暗号化した後、CAモジュール2内に格納されるシステムにおいては、メタデータ作成時に受信したメタデータを元に作成するが、メタデータはメタデータ枠として何度も利用可能なようにメタデータ枠として残しておくこと。

・上記システムにおいて、暗号化コンテンツを視聴するには、蓄積媒体内の暗号化コンテンツを複写し、この複写した暗号化コンテンツを再生する、複写使用により蓄積媒体内の暗号化コンテンツはそのままの状態では保管され、また同時にメタデータも複写して使用することで、家庭内でも受信、蓄積したコンテンツの契約を結ぶ度に視聴でき、家庭内でユーザー特定の蓄積媒体、ICカード等が数種類存在しても本サービス利用が可能となること。

【0083】

【発明の効果】本発明によると、受信端末内で生成した使い捨て鍵を用いてメタデータの作成並びに分割化を行うことで、コンテンツ毎に暗号化可能とする。また、本発明によると、個人を特定できる第2のCAモジュールを合わせることで個人特定のサービスが行うことができる。

【0084】さらに、本発明によると、メタデータ内にコンテンツの所有者情報を入れずにおくことで、コンテンツの譲渡をされた方の受け取り時に初めてコンテンツ

所有者を特定でき、CAモジュールへの所有者情報記入が行なわれることにより、第3者への譲渡目的としたコンテンツサービスが実現可能となる。

【図面の簡単な説明】

【図1】蓄積型テレビ放送サービスの受信側の概要図。

【図2】蓄積型テレビ放送サービスシステムの全体図。

【図3】サービス、イベントの関係の説明図。

【図4】イベント内のコンテンツ構成例の説明図。

【図5】コンテンツに付随する情報の構成図。

【図6】配信時のデータ構成図。

【図7】蓄積型テレビ放送サービスにおける暗号化方式の説明図。

【図8】伝送路暗号とコンテンツ、メタデータ暗号の関係の説明図。

【図9】伝送路における鍵配信方式の説明図。

【図10】ECMを用いたコンテンツ鍵伝送モデルの説明図。

【図11】メタデータの伝送モデルの説明図。

【図12】メタデータを用いたコンテンツ鍵伝送モデルの説明図。

【図13】受信端末の構成図。

【図14】ECMを用いたコンテンツ鍵伝送方式における処理手順の説明図。

【図15】メタデータを用いたコンテンツ鍵伝送方式における処理手順の説明図。

【図16】コンテンツ鍵伝送方式における処理手順1のフローチャート。

【図17】コンテンツ鍵伝送方式における処理手順2のフローチャート。

【図18】リムーバブルメディアへのコンテンツ蓄積処理手順のフローチャート。

【図19】コンテンツ視聴処理手順のフローチャート。

【図20】通常サービスの説明図。

【図21】ギフトサービスの説明図。

【図22】ギフトサービスの伝送路において必要な情報の説明図。

【図23】送信側において暗号化されたコンテンツ、メタデータの暗号形態の説明図。

【図24】ECM又はメタデータを用いた蓄積後視聴のデータの流れについての説明図。

【図25】リムーバブルメディアに蓄積後視聴のデータの流れについての説明図。

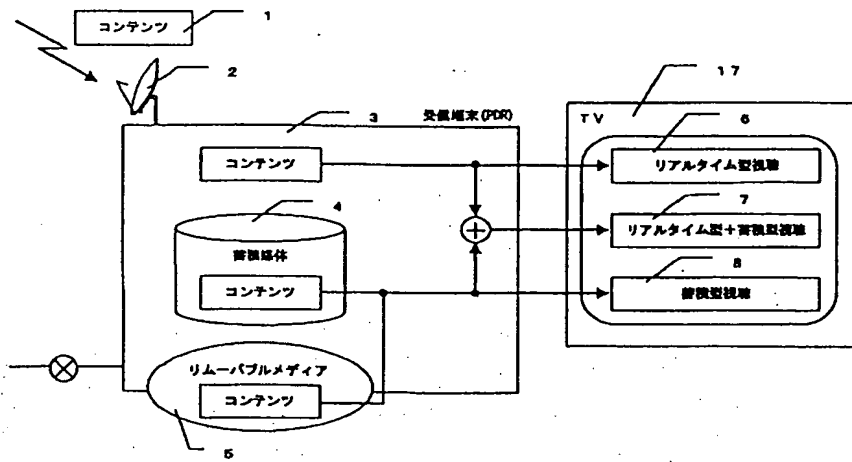
【符号の説明】

1・・・コンテンツ、2・・・アンテナ、3・・・受信端末(PDR)、4・・・蓄積媒体、5・・・リムーバブルメディア、6・・・リアルタイム型視聴、7・・・リアルタイム型+蓄積型視聴、8・・・蓄積型視聴、9・・・センタ側(放送サイド)、10・・・衛星、11・・・外部機器、12・・・受信モジュール、13・・・CPU、14・・・メモリ、15・・・デコーダ、16・・・

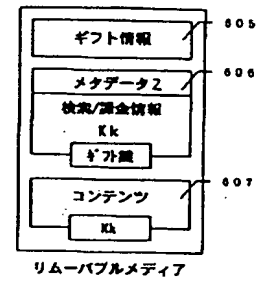
・リムーバブルメディア用ドライブ、17・・・TV、18・・・地上回線、19・・・外部I/F、20・・・イベント、21・・・メインメニュー画面、22・・・映画、23・・・料理、24・・・映像ストリーム、25・・・音声ストリーム、26・・・データストリーム、27・・・中華、28・・・餃子写真、29・・・隠し味、30・・・コンテンツA、31・・・コンテンツB、32・・・コンテンツC、33・・・コンテンツD、34・・・コンテンツE、35・・・サービス、36・・・イベントA、37・・・イベントB、38・・・イベントC、39・・・暗号ありリソース、40・・・暗号なしリソース、41・・・暗号ありストリーム、42・・・暗号なしストリーム、50・・・メタデータ、51・・・メタデータ2A(a)、52・・・メタデータ1A(a)、53・・・全体プロファイル、54・・・個人用プロファイル(a)、55・・・検索用テーブル、56・・・コンテンツA、57・・・メタデータA、58・・・メタデータX、59・・・メタデータ2A(b)、60・・・ES0(デフォルトES)、61・・・ES1(映像ストリーム)、62・・・ES2(音声ストリーム)、63・・・ES3(データストリーム)、64・・・ES4(データカールセル)、65・・・PSI/SI、70・・・暗号化処理部、71・・・暗号化データ(リソース)、72・・・暗号化データ(ストリーム)、73・・・暗号化情報、80・・・ICカード2(a)用、81・・・ICカード2(b)用、100・・・CAモジュール1、101・・・CAモジュール2、200・・・暗号/復号化モジュール、300・・・TSP、301・・・コンテンツ暗号化、302・・・メタデータ暗号化、303・・・伝送路暗号化、310・・・Ks、311・・・イベント暗号化(鍵Ks)、312・・・暗号化イベント、313・・・Kw1、314・・・Ks暗号化(鍵Kw1)、315・・・Ks'、316・・・Km1、317・・・Kw1暗号化(鍵Km1)、318・・・Kw1'、319・・・ECM、320・・・EMM、321・・・Kw1'復号(鍵Km1)、322・・・Ks'復号(鍵Kw1)、323・・・暗号化イベント復号(鍵Ks)、330・・・Kk、331・・・コンテンツ暗号化(鍵Kk)、332・・・暗号化コンテンツ、333・・・Kwc、334・・・Kk暗号化(鍵Kwc)、335・・・Kk'、336・・・Kmc、337・・・Kwc暗号化(鍵Kmc)、338・・・Kwc'、339・・・Kwc'復号(鍵Kmc)、340・・・Kk'復号(鍵Kwc)、34

1・・・暗号化コンテンツ復号(鍵Kk)、350・・・メタデータ暗号化(鍵Kwc)、351・・・暗号化メタデータ、352・・・暗号化メタデータ復号(鍵Kwc)、400・・・配信情報(ECM, EMM)、401・・・配信情報(コンテンツ)、402・・・配信情報(メタデータ)、403・・・RAM、404・・・HDD蓄積前処理、405・・・HDD蓄積前メタデータ、406・・・HDD蓄積前コンテンツ、407・・・HDD蓄積コンテンツ、メタデータ、408・・・メタデータ(コピー)、409・・・コンテンツ(コピー)、410・・・検索テーブル、411・・・HDD、412・・・検索処理、413・・・メタデータ復号、414・・・復号メタデータ、415・・・契約手続き、416・・・課金処理、417・・・メタデータ(契約情報)作成、418・・・メタデータ分離処理、419・・・メタデータ2暗号化、420・・・メタデータ2(HDD内)、421・・・メタデータ2(リムーバブルメディア内)、422・・・メタデータ1、K1'暗号化、424・・・Km2、425・・・暗号化メタデータ、K1'、450・・・配信情報(EMM)、451・・・配信情報(メタデータ)、452・・・RAM、453・・・HDD蓄積前処理、500・・・スクランブル復号、501・・・Kk'復号、502・・・Kk入手、503・・・メタデータ復号、504・・・検索テーブル情報追加、505・・・メタデータKk記入、506・・・K1生成、507・・・メタデータ暗号化、508・・・コンテンツ、メタデータ蓄積、520・・・HDD検索、521・・・蓄積コンテンツ選択、522・・・メタデータ復号、523・・・契約条件確認・記入、蓄積選択、524・・・課金処理、525・・・契約情報作成、526・・・メタデータ分離、527・・・K1'生成、528・・・メタデータ2暗号化、529・・・リムーバブルメディア蓄積処理(メタデータ2)、530・・・メタデータ1、K1'暗号化、531・・・CAモジュール蓄積、532・・・リムーバブルメディアにコンテンツ蓄積、540・・・視聴コンテンツ選択、541・・・契約条件確認・記入、視聴選択、542・・・HDD蓄積、543・・・コンテンツ復号、600・・・ユーザー、601・・・送り主、602・・・受け取り主、603・・・伝送路、604・・・受け取り主側CAモジュール2、605・・・ギフト情報、606・・・メタデータ、607・・・暗号化コンテンツ。

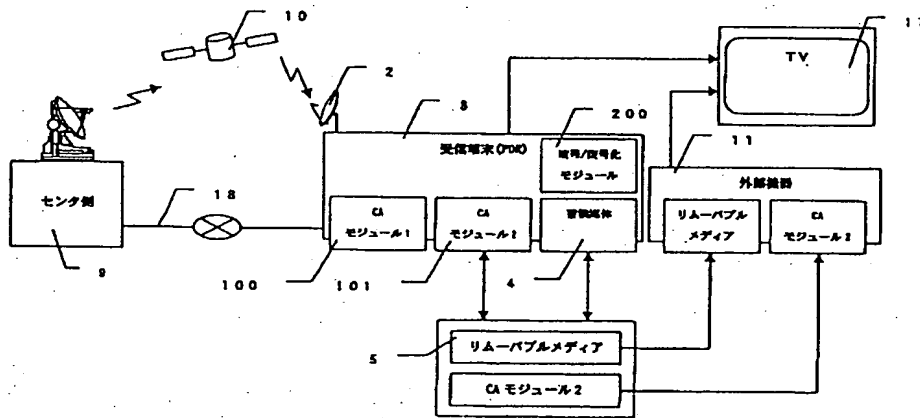
【図1】



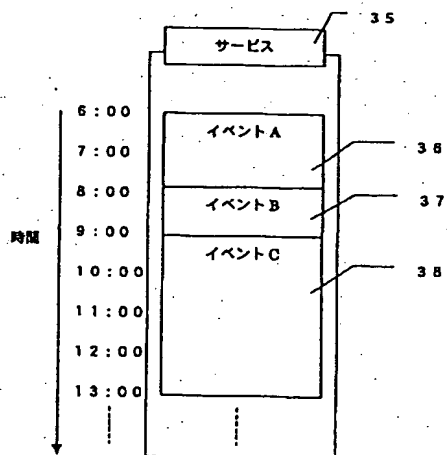
【図22】



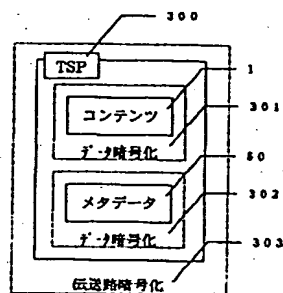
【図2】



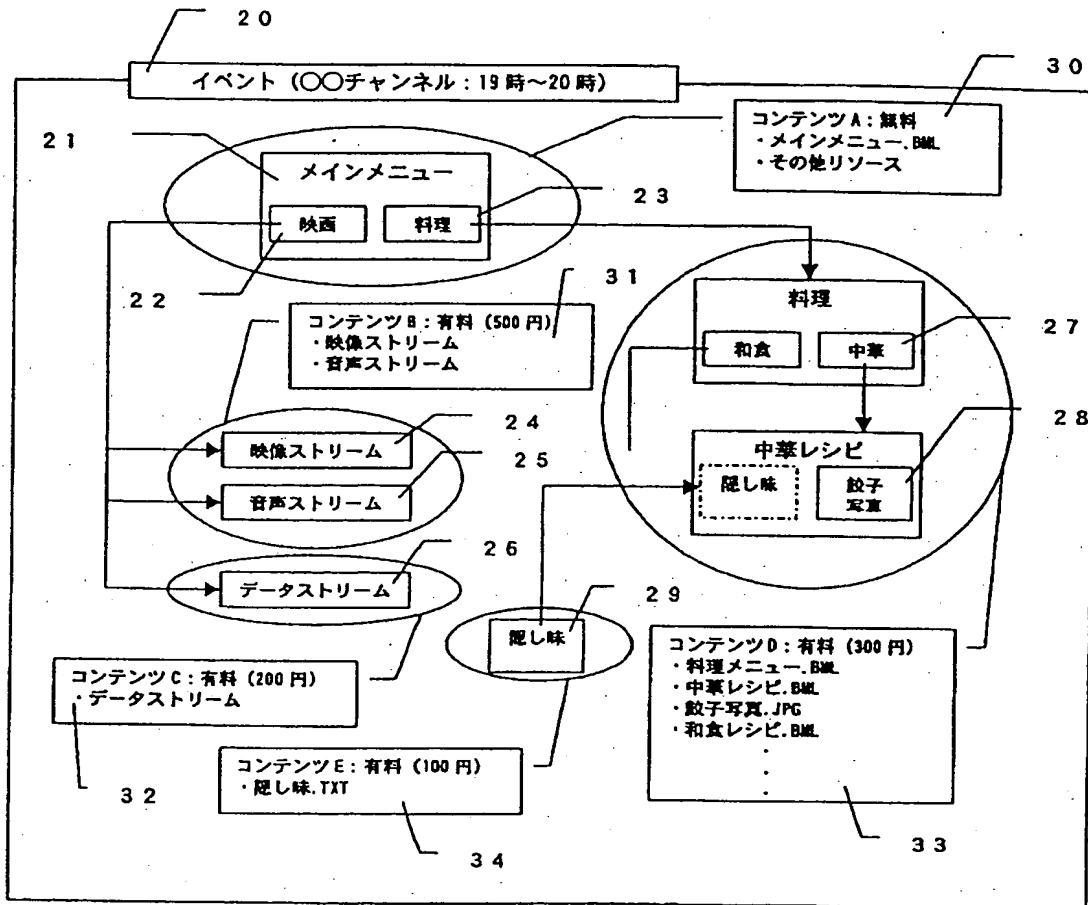
【図3】



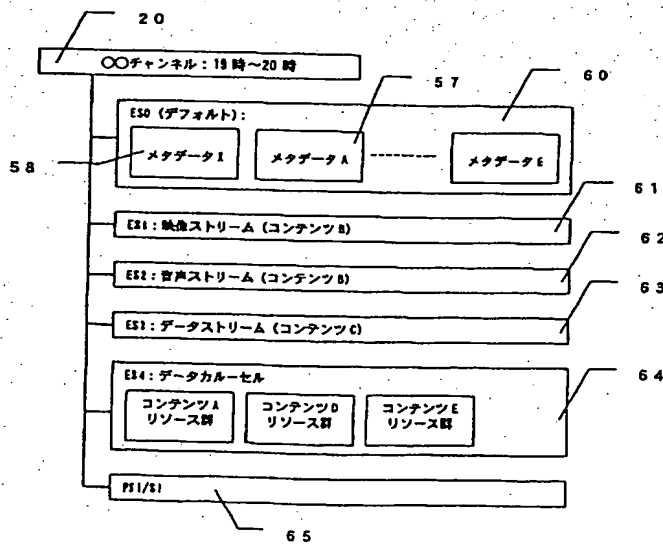
【図8】



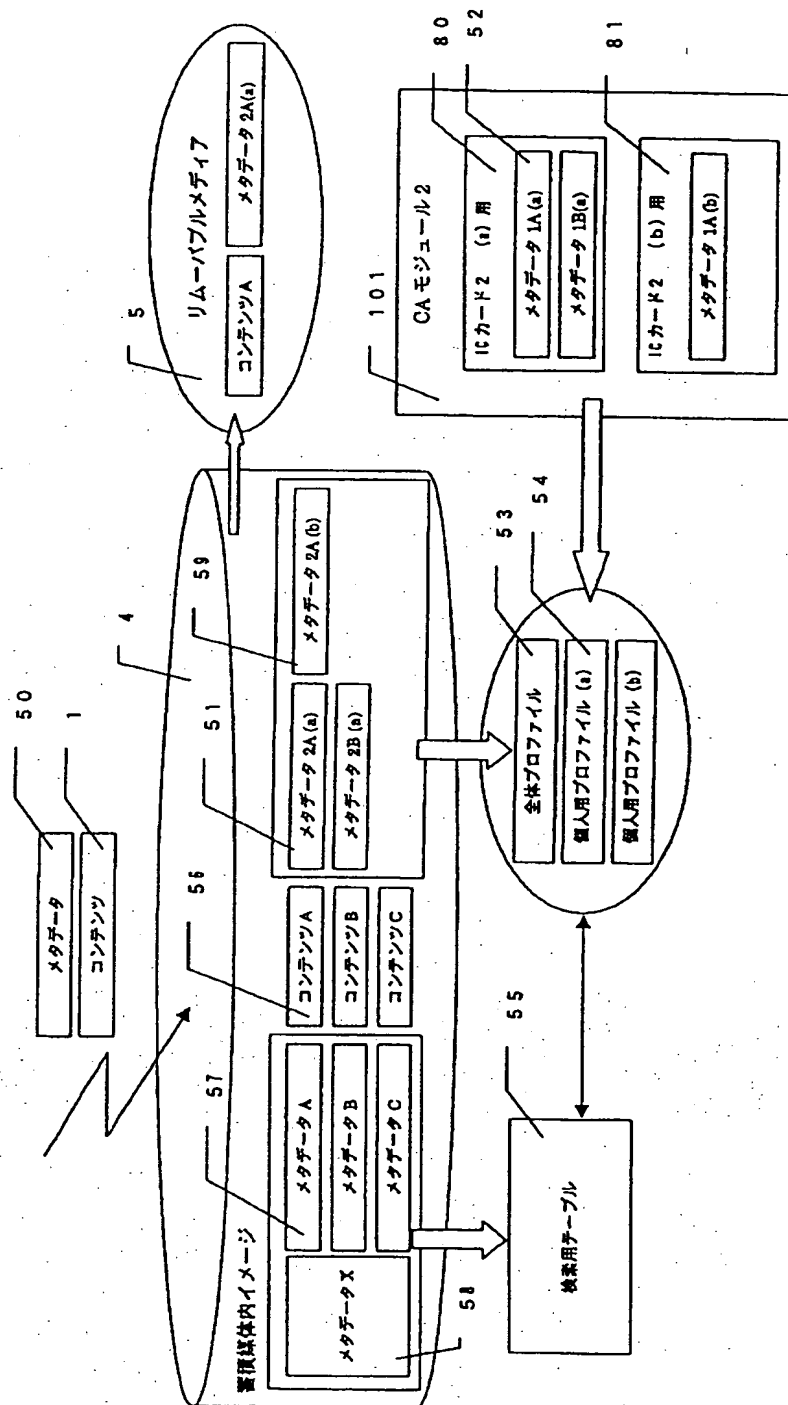
【図4】



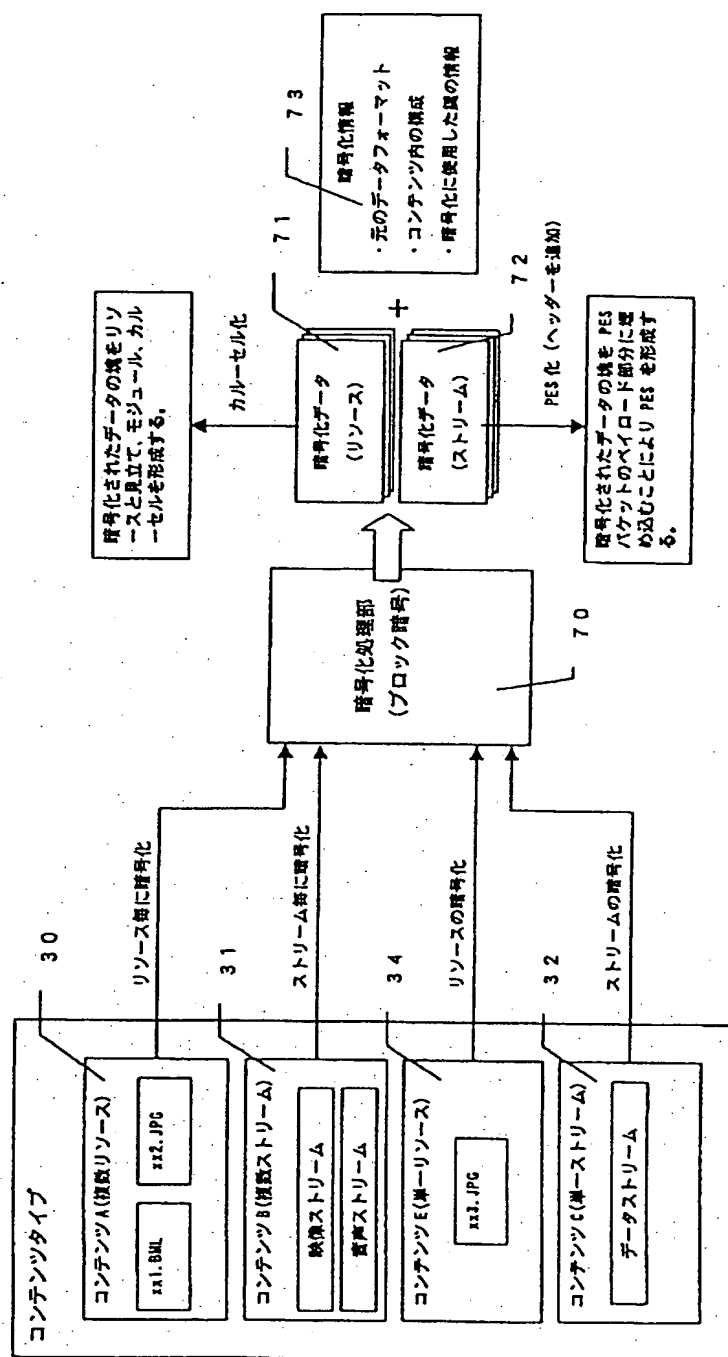
【図6】



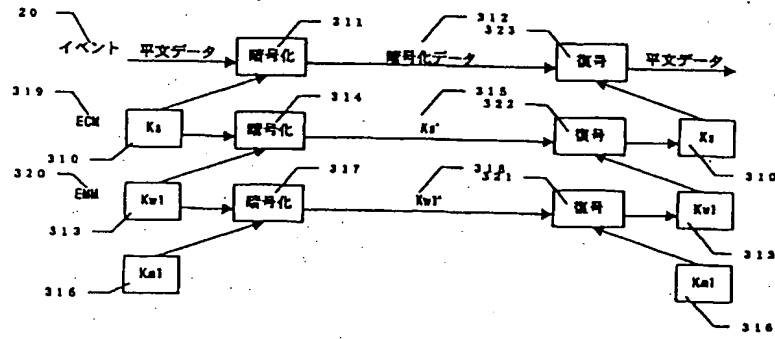
【図5】



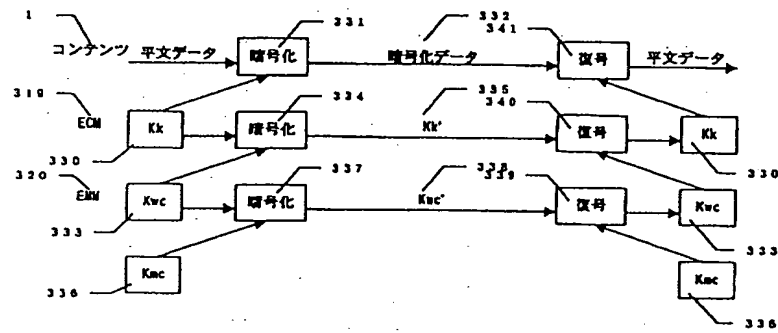
【図 7】



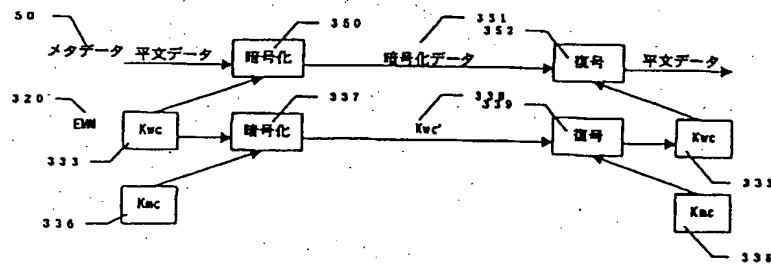
【図9】



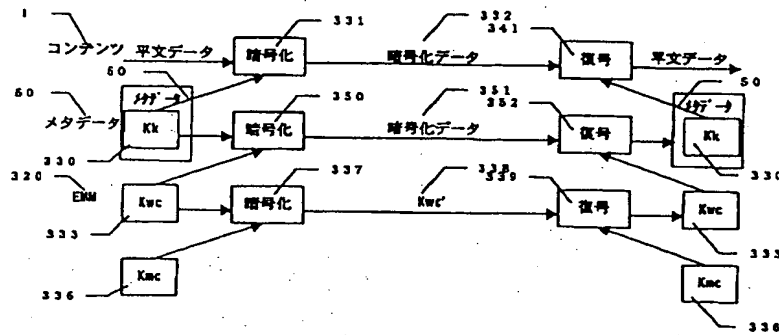
【図10】



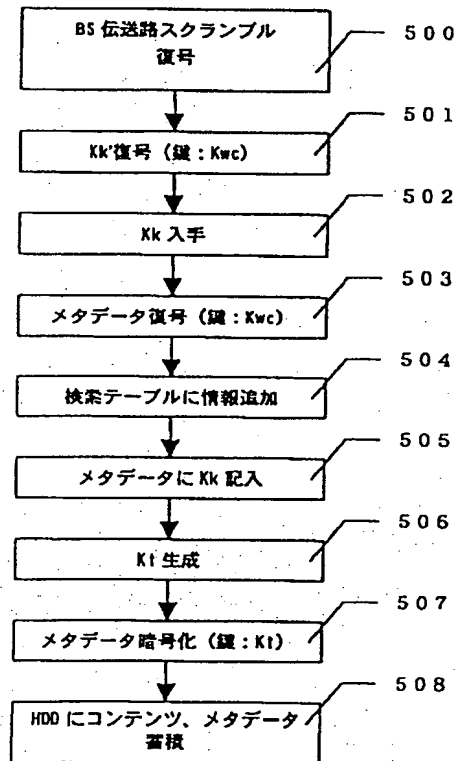
【図11】



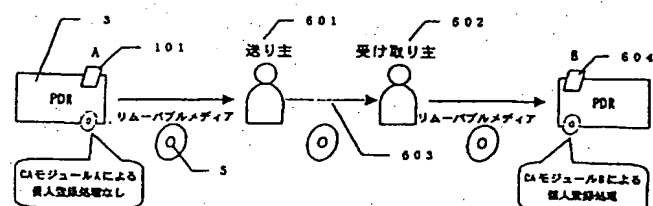
【図12】



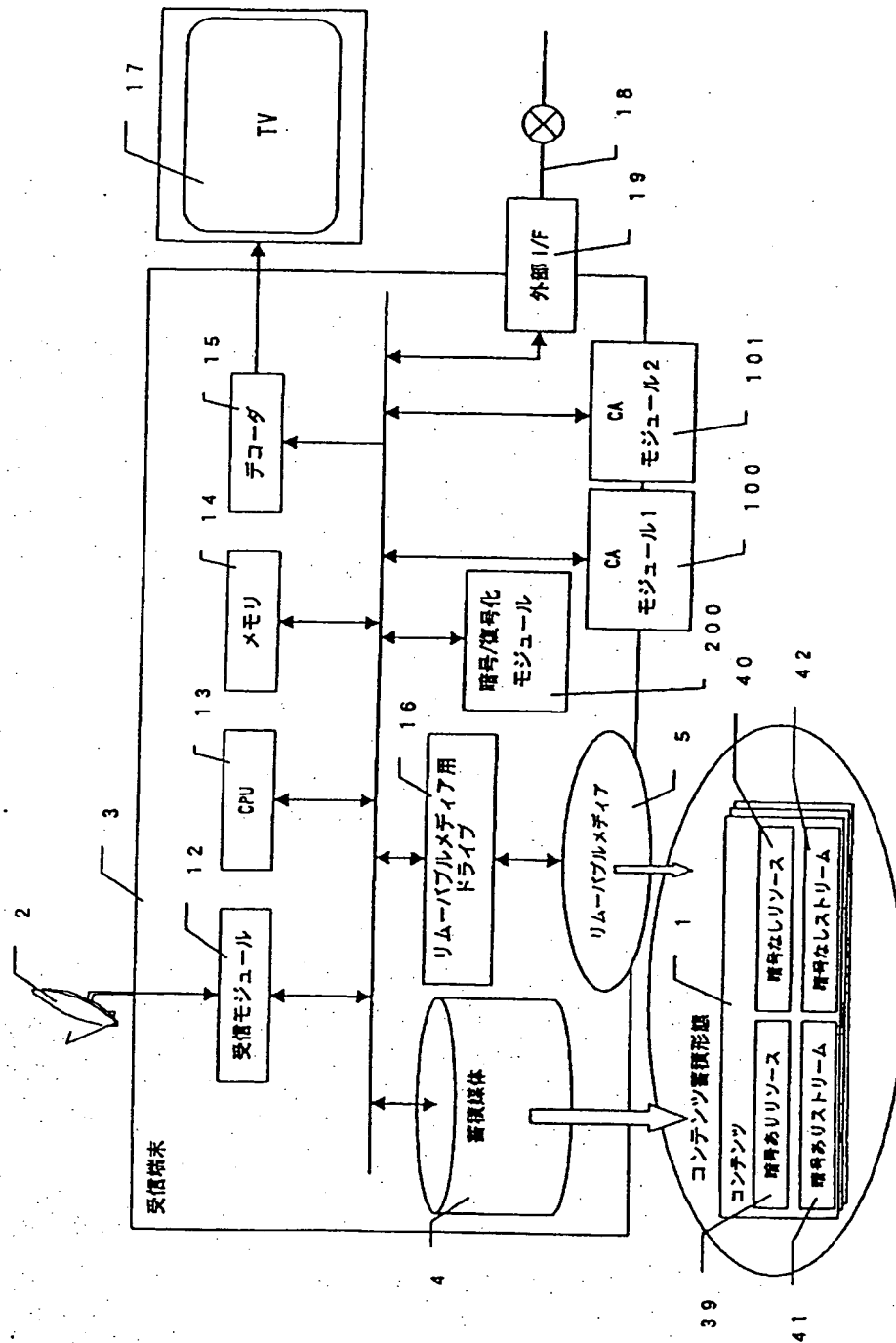
【図16】



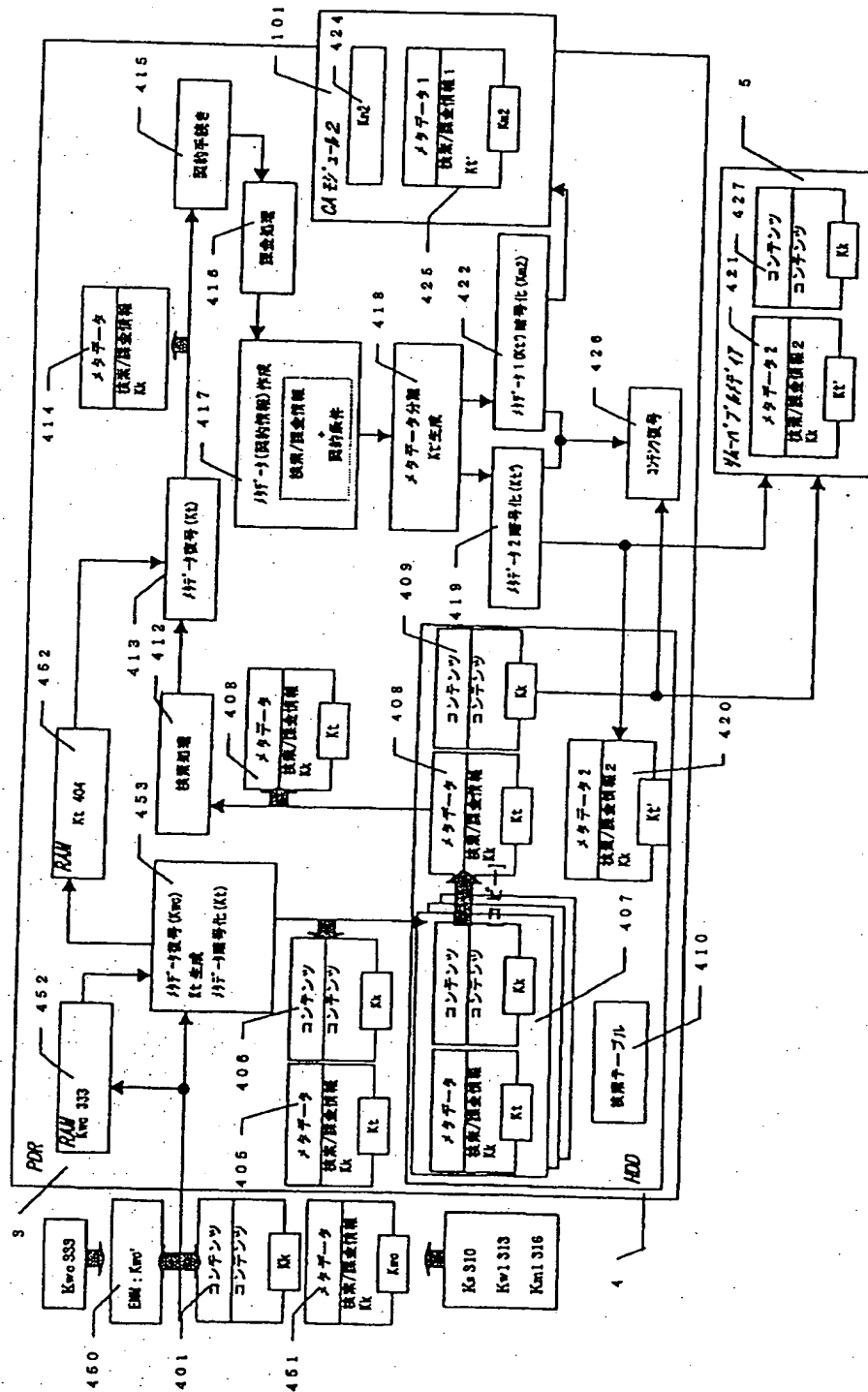
【図21】



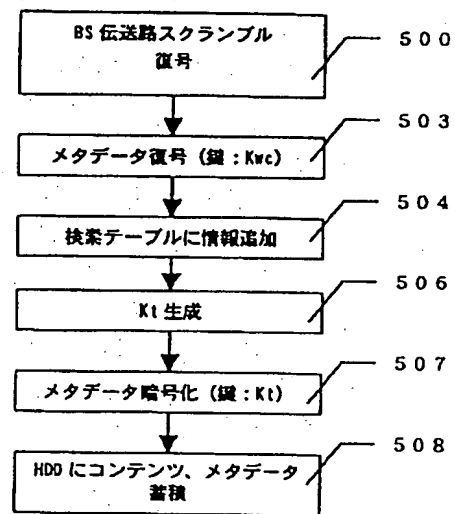
【図13】



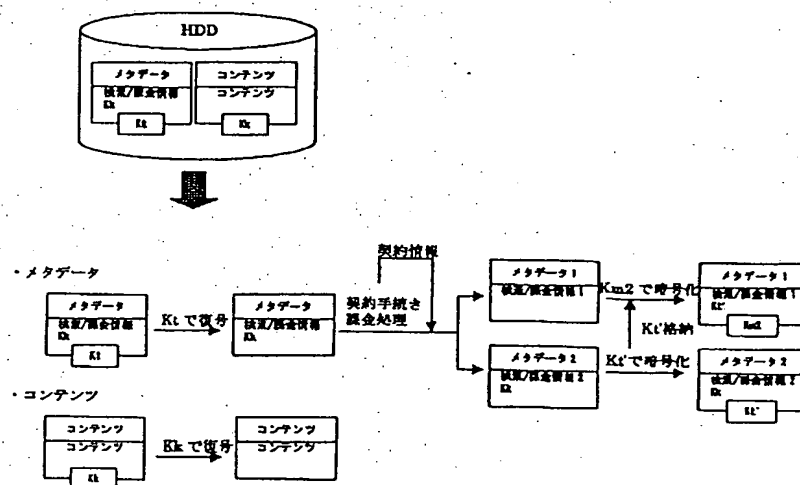
【圖 15】



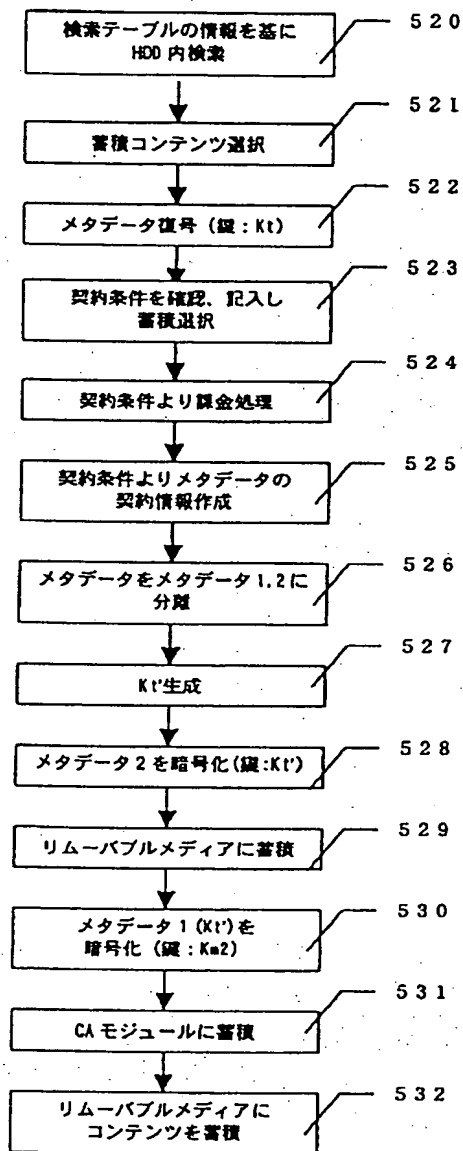
【図17】



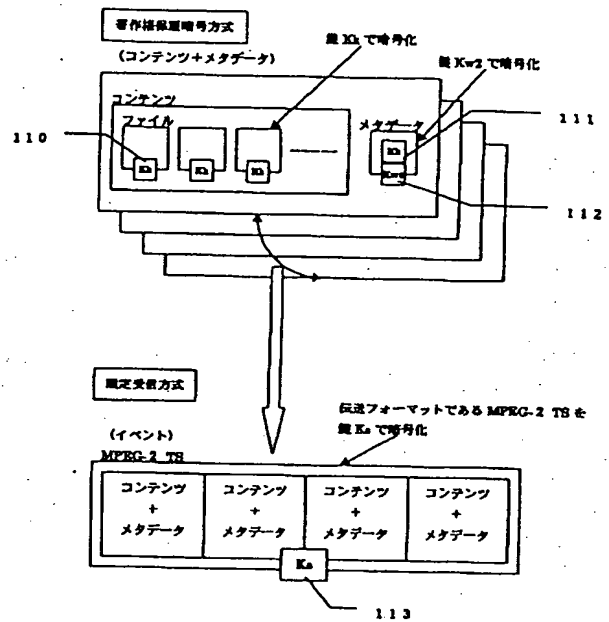
【図24】



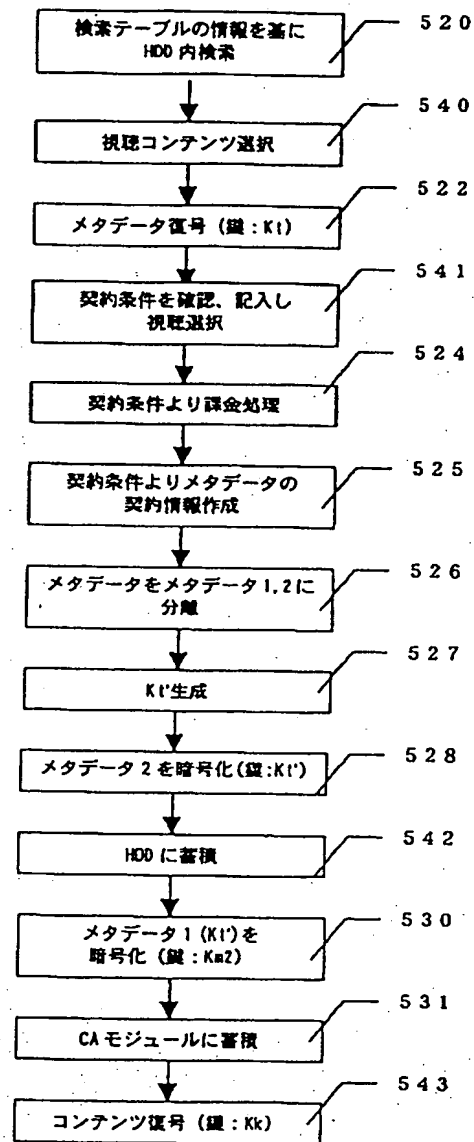
【図18】



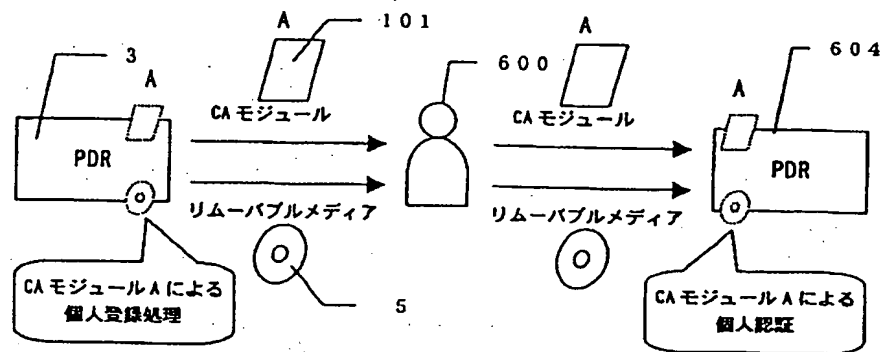
【図23】



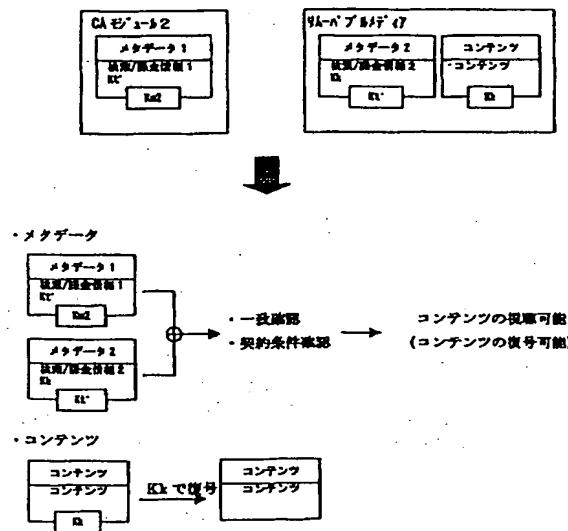
【図19】



【図20】



【図 25】



フロントページの続き

(51) Int. Cl. 7

H 0 4 N 7/16
7/167

識別記号

F I

H 0 4 N 5/91

7/167

テ-マ-ド (参考)

L
P
Z

(72) 発明者 山崎 伊織

東京都千代田区神田駿河台四丁目6番地
株式会社日立製作所放送・通信システム推
進事業部内

Fターム(参考) 5C025 BA25 BA27 BA28 BA30 DA01
DA04 DA10
5C053 FA20 FA23 FA24 GA20 LA07
LA14
5C064 BA07 BB01 BB02 BC10 BC17
BC20 BD08 BD09 CA14 CB01
CC04 CC06
5J104 AA16 AA34 DA04 EA04 EA17
JA03 NA02 PA14